日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年　６月１４日

出願番号
Application Number: 特願２００２－１７４８８３

[ST. 10/C]: [ＪＰ２００２－１７４８８３]

出願人
Applicant(s): 松下電器産業株式会社

２００３年　７月１１日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０５６６８３

【書類名】　特許願

【整理番号】　2037840026

【提出日】　平成14年 6月14日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 12/14

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　難波　剛

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　中井　勝博

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　平野　雄久

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　手塚　智明

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100081813

【弁理士】

【氏名又は名称】　早瀬　憲一

【電話番号】　06(6395)3251

【手数料の表示】

【予納台帳番号】　013527

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9600402

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　半導体集積回路装置

【特許請求の範囲】

【請求項１】　半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記第２の格納手段は、該半導体集積回路外部から読出しが可能な外部読出し可能領域と、読出しが不可能な外部読出し不可能領域とを有するものであり、

上記第２の格納手段の外部読出し可能領域に任意のデータを入力格納したのち、該データを該半導体集積回路の外部に読出して、該任意のデータが上記入力した通りのデータであるかを確認し、そののち、上記第１の格納手段からの上記書き換えプログラムを、上記第２の格納手段の外部読出し不可能領域に格納するようにした、

ことを特徴とする半導体集積回路装置。

【請求項２】　半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記第２の格納手段に格納された上記書き換えプログラムの特定部分のみを読み出すように制御する制御回路を備えた、

ことを特徴とする半導体集積回路装置。

【請求項３】　請求項２に記載の半導体集積回路装置において、

上記制御回路は、上記第２の格納手段の特定のアドレスにある書き換えプログラムのみを読み出すように制御するものとした、

ことを特徴とする半導体集積回路装置。

【請求項４】　請求項２に記載の半導体集積回路装置において、

上記制御回路は、上記第２の格納手段に格納した書き換えプログラムの特定のビットのみを読み出すように制御するものとした、

ことを特徴とする半導体集積回路装置。

【請求項５】　半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記書き換えプログラムは、書き換え後に該プログラムの一部を実行するプログラムを含んだものであり、

上記第２の格納手段に格納した上記書き換えプログラムの一部を実行する、

ことを特徴とする半導体集積回路装置。

【請求項６】　請求項５に記載の半導体集積回路装置において、

上記実行する書き換えプログラムの一部は、非連続なプログラム領域を順次実行するものである、

ことを特徴とする半導体集積回路装置。

【請求項７】　半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記半導体集積回路内に、上記第１の格納手段から上記第２の格納手段に転送される上記書き換えプログラムを監視する転送監視手段を備えた、

ことを特徴とする半導体集積回路装置。

【請求項８】　半導体集積回路内の演算処理ユニットにコンテンツを処理す

る動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記書き換えプログラムは、プログラムの正誤の判定を行うチェックプログラムが含まれたものであり、

上記半導体集積回路内に、上記演算処理ユニットのワークメモリと、

上記第２の格納手段または上記ワークメモリと、上記演算処理ユニットのプログラム入力またはデータ入力との接続を切り替える接続切り替え手段とを備え、

上記第２の格納手段に格納された上記書き換えプログラムから抽出した上記チェックプログラムを上記ワークメモリに格納し、該ワークメモリに格納したチェックプログラムにより、上記演算処理ユニットを動作させ、上記書き換えプログラムの正誤チェックを行う、

ことを特徴とする半導体集積回路装置。

【請求項９】　請求項８に記載の半導体集積回路装置において、

上記第２の格納手段は、上記書き換えプログラムを格納するとともに、該書き換えプログラムのうち、ある決められたかたまりから所定の法則に従い一意に得られるデータを格納するものとした、

ことを特徴とする半導体集積回路装置。

【請求項１０】　請求項９に記載の半導体集積回路装置において、

上記一意に得られるデータを、上記プログラムの正誤チェックをするためのチェックコードとして使用する、

ことを特徴とする半導体集積回路装置。

【請求項１１】　請求項８に記載の半導体集積回路装置において、

上記第２の格納手段は、その構成を、上記書き換えプログラムが格納されていない領域を順次２分割した構成とし、該２分割した各々の領域に同じプログラムデータを格納するものであり、

上記チェックプログラムは、上記２分割した両領域の各々に格納された同じプ

ログラムデータを比較して正誤を判定するプログラムと、

前回の判定結果が正しいと判定されたときに、前回２分割した領域の１方の領域を、プログラムが格納されていない領域としてさらに２分割し、該分割した領域の各々に同じプログラムデータを格納する動作を繰り返すプログラムとを有し、

上記第２の格納手段に格納すべきプログラムすべてを順次格納する、

ことを特徴とする半導体集積回路装置。

【請求項１２】　請求項１１に記載の半導体集積回路装置において、

上記第２の格納手段は、該第２の格納手段の上記書き換えプログラムが格納されていない領域を順次２分割した各々の領域に、上記書き換えプログラムデータと、該プログラムデータから所定の法則に従い一意に得られるデータとを格納するものとした、

ことを特徴とする半導体集積回路装置。

【請求項１３】　請求項１２に記載の半導体集積回路装置において、

上記一意に得られるデータが、該プログラムデータの反転データである、

ことを特徴とする半導体集積回路装置。

【請求項１４】　請求項８ないし１３のいずれかに記載の半導体集積回路装置において、

上記チェックプログラムを予め格納したＲＯＭ（Read Only Memory）を備え、

上記ＲＯＭにより上記演算処理ユニットを動作させて、上記書き換えプログラムの正誤チェックを行う、

ことを特徴とした半導体集積回路装置。

【請求項１５】　請求項１ないし１４のいずれかに記載の半導体集積回路装置において、

上記半導体集積回路内に、暗号化された書き換えプログラムを復号する復号化手段を備え、

上記第１の格納手段に格納された書き換えプログラムが予め暗号化されている場合、上記復号化手段は、該暗号化プログラムを復号化し、上記第２の格納手段に復号化した上記書き換えプログラムを格納する、

ことを特徴とする半導体集積回路装置。

【請求項１６】　半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である、予め暗号化された書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記半導体集積回路内に、上記第１の格納手段からの上記暗号化された書き換えプログラムを復号化し、該復号化した書き換えプログラムを上記第２の格納手段に転送する復号化手段と、

上記第２の格納手段に格納した書き換えプログラムを再度暗号化する暗号化手段とを備え、

上記暗号化手段で暗号化された書き換えプログラムと上記第１の格納手段に保持している暗号化された書き換えプログラムとを比較する、

ことを特徴とする半導体集積回路装置。

【請求項１７】　請求項１１ないし１３、及び１６のいずれかに記載の半導体集積回路装置において、

上記第２の格納手段にデータが正しく格納されていない場合、不良箇所を検出し、上記第１の格納手段に保持した書き換えプログラムを修正可能とした、

ことを特徴とする半導体集積回路装置。

【請求項１８】　請求項１ないし１７のいずれかに記載の半導体集積回路装置において、

当該半導体集積回路装置外部に保持した書き換えプログラムを、上記半導体集積回路内にダウンロード可能とした、

ことを特徴とする半導体集積回路装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は半導体集積回路装置に関するものであり、特に、内容が第三者へ漏洩

したくない機密情報であるプログラムの保護に関するものである。

【０００２】

【従来の技術】

ＤＳＰやＣＰＵなどの演算処理ユニットを含む半導体集積回路において、演算処理ユニットのプログラムは、コスト面やプログラムの機密性を保つという点においてはＲＯＭとしてプログラムを格納することが有利となる。しかしながら、ＲＯＭなどの書き換え不可能な手段でプログラムを保持した場合、仕様変更やプログラム自身の不具合に柔軟な対応が取りにくい。このような回路の開発における容易さなどの点から、プログラムを半導体集積回路内部に格納する手段をＲＡＭなどの書き換え可能な手段として所有することがある。このような構成を持つ回路においては、ＤＳＰやＣＰＵのような信号処理・機器の制御を担う演算処理ユニットなどに必要なプログラムを事前に書き換え可能なＲＡＭなどの指定領域にダウンロードする必要があった。

【０００３】

しかし、ＤＳＰやＣＰＵなどの演算処理ユニットのプログラムを外部からＲＡＭにダウンロードする半導体集積回路においては、プログラムを半導体集積回路内部にＲＯＭで持っている場合よりもプログラムの内容が第三者に漏洩する危険が高いという欠点を有していた。

例えば、半導体集積回路外部に保持するプログラムが著作権保護を目的として策定されたウォーターマーク（電子透かし）を検出するためのプログラムのような場合、プログラムの内容が悪意を持った第三者に漏洩したことによって、著作権保護のための仕組みを無効化される恐れがあるため、プログラム自身を保護する必要がある。

この場合、半導体集積回路内にダウンロードするプログラムを予め暗号化させて、該半導体集積回路内で復号化させることにより、プログラム自身を保護することが考えられる。

【０００４】

【発明が解決しようとする課題】

しかしながら、この予め暗号化したデータ、及び非暗号化データも含めて半導

体集積回路内の書き換え可能な領域にダウンロードしたプログラムデータが正しく格納できたか否かを、機密性を保持しながら確認することは困難である。

本発明はこのような問題を解決するためになされたものであり、機密性を要するプログラムデータを外部に漏らすことなく、正しくダウンロードできたか否かを確認できる半導体集積回路装置を提供することを目的とする。

【０００５】

【課題を解決するための手段】

上記問題を解決するために、本発明の請求項１に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記第２の格納手段は、該半導体集積回路外部から読出しが可能な外部読出し可能領域と、読出しが不可能な外部読出し不可能領域とを有するものであり、上記第２の格納手段の外部読出し可能領域に任意のデータを入力格納したのち、該データを該半導体集積回路の外部に読出して、該任意のデータが上記入力した通りのデータであるかを確認し、そののち、上記第１の格納手段からの上記書き換えプログラムを、上記第２の格納手段の外部読出し不可能領域に格納するようにしたものである。

【０００６】

これにより、例えばダミーデータなどを、上記第２の格納手段の読み出し可能な領域に書き込んで、該書き込んだダミーデータを読み出してチェックをすることにより、半導体集積回路内に正しく上記書き換えプログラムが格納されたかどうかを、該書き換えプログラムの機密性を保持しながら確認することができる。

【０００７】

また、本発明の請求項２に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納

手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記第２の格納手段に格納された上記書き換えプログラムの特定部分のみを読み出すように制御する制御回路を備えたものである。

【０００８】

これにより、上記第２の格納手段に格納された特定部分のみを読み出して、該特定部分を検証することにより、上記書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

【０００９】

また、本発明の請求項３に記載の半導体集積回路装置は、請求項２に記載の半導体集積回路装置において、上記制御回路は、上記第２の格納手段の特定のアドレスにある書き換えプログラムのみを読み出すように制御するものとしたものである。

【００１０】

これにより、上記第２の格納手段の特定のアドレスのみを読み出して、該特定のアドレスのデータを検証することにより、上記書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

【００１１】

また、本発明の請求項４に記載の半導体集積回路装置は、請求項２に記載の半導体集積回路装置において、上記制御回路は、上記第２の格納手段に格納した書き換えプログラムの特定のビットのみを読み出すように制御するものとしたものである。

【００１２】

これにより、上記第２の格納手段の特定のビットのみを読み出して、該特定のビットのみを検証することにより、上記書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持し

ながら確認することができる。

【００１３】

また、本発明の請求項５に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記書き換えプログラムは、書き換え後に該プログラムの一部を実行するプログラムを含んだものであり、上記第２の格納手段に格納した上記書き換えプログラムの一部を実行するものである。

【００１４】

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

【００１５】

また、本発明の請求項６に記載の半導体集積回路装置は、請求項５に記載の半導体集積回路装置において、上記実行する書き換えプログラムの一部は、非連続なプログラム領域を順次実行するものである。

【００１６】

これにより、例えば、上記第２の格納手段に格納された上記書き換えプログラムの先頭プログラムと最終プログラムとを実行した場合、該書き換えプログラムが最後まで正しく格納できたかを、該書き換えプログラムの機密性を保持しながら確認することができる。

【００１７】

また、本発明の請求項７に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理

する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記半導体集積回路内に、上記第１の格納手段から上記第２の格納手段に転送される上記書き換えプログラムを監視する転送監視手段を備えたものである。

【００１８】

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

【００１９】

また、本発明の請求項８に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記書き換えプログラムは、プログラムの正誤の判定を行うチェックプログラムが含まれたものであり、上記半導体集積回路内に、上記演算処理ユニットのワークメモリと、上記第２の格納手段または上記ワークメモリと、上記演算処理ユニットのプログラム入力またはデータ入力との接続を切り替える接続切り替え手段とを備え、上記第２の格納手段に格納された上記書き換えプログラムから抽出した上記チェックプログラムを上記ワークメモリに格納し、該ワークメモリに格納したチェックプログラムにより、上記演算処理ユニットを動作させ、上記書き換えプログラムの正誤チェックを行うものである。

【００２０】

これにより、接続切り換え手段にて演算処理ユニットのプログラム入力またはデータ入力を切り替えて、上記書き換えプログラムのデータを取り込んで、例えば該書き換えプログラムデータのチェックサムなどをとって、予め決めておいた値と比較することが可能になるので、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該

書き換えプログラムの機密を保持しながら確認することができる。

【００２１】

また、本発明の請求項９に記載の半導体集積回路装置は、請求項８に記載の半導体集積回路装置において、上記第２の格納手段は、上記書き換えプログラムを格納するとともに、該書き換えプログラムのうち、ある決められたかたまりから所定の法則に従い一意に得られるデータを格納するものとしたものである。

【００２２】

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第２の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる。

【００２３】

また、本発明の請求項１０に記載の半導体集積回路装置は、請求項９に記載の半導体集積回路装置において、上記一意に得られるデータを、上記プログラムの正誤チェックをするためのチェックコードとして使用するものである。

【００２４】

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第２の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる。

【００２５】

また、本発明の請求項１１に記載の半導体集積回路装置は、請求項８に記載の半導体集積回路装置において、上記第２の格納手段は、その構成を、上記書き換えプログラムが格納されていない領域を順次２分割した構成とし、該２分割した各々の領域に同じプログラムデータを格納するものであり、上記チェックプログラムは、上記２分割した両領域の各々に格納された同じプログラムデータを比較して正誤を判定するプログラムと、前回の判定結果が正しいと判定されたときに

、前回２分割した領域の１方の領域を、プログラムが格納されていない領域としてさらに２分割し、該分割した領域の各々に同じプログラムデータを格納する動作を繰り返すプログラムとを有し、上記第２の格納手段に格納すべきプログラムすべてを順次格納するものである。

【００２６】

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第２の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる。

【００２７】

また、本発明の請求項１２に記載の半導体集積回路装置は、請求項１１に記載の半導体集積回路装置において、上記第２の格納手段は、該第２の格納手段の上記書き換えプログラムが格納されていない領域を順次２分割した各々の領域に、上記書き換えプログラムデータと、該プログラムデータから所定の法則に従い一意に得られるデータとを格納するものとしたものである。

【００２８】

これにより、例えば、第２の格納手段の前段に復号化回路を備えて、該復号化回路の不具合により出力が固定値になり、排他的論理和をとってもデータが一致し、上記第２の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、第２の格納手段に格納した書き換えプログラムの誤りを容易に見つけ出すことができる。

【００２９】

また、本発明の請求項１３に記載の半導体集積回路装置は、請求項１２に記載の半導体集積回路装置において、上記一意に得られるデータが、該プログラムデータの反転データであるものとしたものである。

【００３０】

これにより、例えば、第２の格納手段の前段に復号化回路を備えて、該復号化回路の不具合により出力が固定値になり、排他的論理和をとってもデータが一致

し、上記第２の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、第２の格納手段に格納した書き換えプログラムの誤りを容易に見つけ出すことができる。

【００３１】

また、本発明の請求項１４に記載の半導体集積回路装置は、請求項８ないし１３のいずれかに記載の半導体集積回路装置において、上記チェックプログラムを予め格納したＲＯＭ（Read Only Memory）を備え、上記ＲＯＭにより上記演算処理ユニットを動作させて、上記書き換えプログラムの正誤チェックを行うものである。

【００３２】

これにより、上記チェックプログラムの転送誤り等により、チェックプログラムが機能しなくなるのを防ぎ、上記第２の格納手段に上記書き換えプログラムが正しく格納できたか否かを確認するチェックプログラムを安定的に提供することができる効果がある。

【００３３】

また、本発明の請求項１５に記載の半導体集積回路装置は、請求項１ないし１４のいずれかに記載の半導体集積回路装置において、上記半導体集積回路内に、暗号化された書き換えプログラムを復号する復号化手段を備え、上記第１の格納手段に格納された書き換えプログラムが予め暗号化されている場合、上記復号化手段は、該暗号化プログラムを復号化し、上記第２の格納手段に復号化した上記書き換えプログラムを格納するものである。

【００３４】

これにより、第三者に漏洩したくない機密情報であり、また、予め暗号化されている書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

【００３５】

また、本発明の請求項１６に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格

納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である、予め暗号化された書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記半導体集積回路内に、上記第１の格納手段からの上記暗号化された書き換えプログラムを復号化し、該復号化した書き換えプログラムを上記第２の格納手段に転送する復号化手段と、上記第２の格納手段に格納した書き換えプログラムを再度暗号化する暗号化手段とを備え、上記暗号化手段で暗号化された書き換えプログラムと上記第１の格納手段に保持している暗号化された書き換えプログラムとを比較するものである。

【００３６】

これにより、第三者に漏洩したくない機密情報であり、また、予め暗号化されている書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

【００３７】

また、本発明の請求項１７に記載の半導体集積回路装置は、請求項１１ないし１３、及び１６のいずれかに記載の半導体集積回路装置において、上記第２の格納手段にデータが正しく格納されていない場合、不良箇所を検出し、上記第１の格納手段に保持した書き換えプログラムを修正可能としたものである。

【００３８】

これにより、第２の格納手段において正しく格納できなかった箇所を使用しないように書き換えプログラムを修正して書き込むので、メモリを有効に活用することができる。

【００３９】

また、本発明の請求項１８に記載の半導体集積回路装置は、請求項１ないし１７のいずれかに記載の半導体集積回路装置において、当該半導体集積回路装置外部に保持した書き換えプログラムを、上記半導体集積回路内にダウンロード可能としたものである。

【００４０】

これにより、書き換えプログラムを半導体集積回路装置外部に有する場合にお

いても、ネットワーク等の通信手段を用いてダウンロードでき、第三者に漏洩したくない機密情報である書き換えプログラムが正しく格納できたか否かを、機密性を保持しながら確認することができる。

【００４１】

【発明の実施の形態】

以下、本発明の実施の形態について、図を用いて説明する。

（実施の形態１）

図１は、本発明の実施の形態１に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムをダウンロードする例を示す。

【００４２】

図において、１００は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であり、１０５は制御用マイコン、１０１はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第１の格納手段）である。半導体集積回路１０９は、暗号化された書き換えプログラムを復号化するための復号化回路（複号化手段）１０２と、書き換え可能なＲＡＭ（第２の格納手段）１０８と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ１０７の処理を行う演算処理回路（演算処理ユニット）１０６とから構成される。

【００４３】

また、本発明の実施の形態１に係る半導体集積回路装置において、書き換え可能なＲＡＭ１０８は、半導体集積回路１０９の外部から読み出し可能な外部読出し可能領域１０３と、半導体集積回路１０９の外部から読み出し不可能な外部読出し不可能領域１０４とから構成される。

【００４４】

以上のように構成された半導体集積回路装置１００について、図２のフローチャートを用いてその動作を説明する。

制御用マイコン１０５の制御にしたがい、暗号化されていないデータを書き換え可能なＲＡＭ１０８の外部読出し可能領域１０３に入力する（ステップＳ２０１）。次に、外部読出し可能領域１０３に入力したデータが正しいかを半導体集

積回路１０９外部に読み出して制御用マイコン１０５等でチェックする（ステップＳ２０２）。ステップＳ２０２でチェックした結果が正しい場合に、制御用マイコン１０５の制御にしたがいメモリ１０１の暗号化された書き換えプログラムを復号化回路１０２に入力し（ステップＳ２０３）、暗号化された書き換えプログラムを復号する（ステップＳ２０４）。次に、ステップＳ２０４で復号化された書き換えプログラムを書き換え可能なＲＡＭ１０８の外部読出し不可能領域１０４に入力する（ステップＳ２０５）。以上の処理により、第三者に漏洩したくない書き換えプログラムの機密性を保ちながら、該書き換えプログラムが正しく格納されているか否かをチェックすることができる。

なお、書き換え可能なＲＡＭ１０９の外部読出し可能領域１０３に格納するデータは、半導体集積回路装置の内部、及び外部のどちらに用意してもよく、チェック用のデータであればよい。

【００４５】

以上のような、本発明の実施の形態１に係る半導体集積回路装置は、第三者に漏洩したくない機密情報である書き換えプログラムを書き換え可能なＲＡＭ１０８に入力する場合に、該ＲＡＭ１０８に設けた外部読出し可能領域１０３、及び外部読出し不可能領域１０４のうち、外部読み出し可能領域１０３にチェック用のデータを格納し、該データのチェックの結果が正しいと判定された後、外部読出し不可能領域１０４に該機密情報のプログラムを格納することにより、第三者に漏洩したくない機密情報である書き換えプログラムを格納したＲＡＭ１０８の製造上の欠陥、及び入力するまでの経路のチェックをすることができる。

【００４６】

（実施の形態２）

本発明の実施の形態２に係る半導体集積回路装置は、第三者に漏洩したくない機密情報である書き換えプログラムの機密性を保ちながら、該書き換えプログラムが半導体集積回路内の書き換え可能なＲＡＭに正しく格納されているかを確認するために、格納した書き換えプログラムの特定部分のみを半導体集積回路に読み出すように制御する制御回路を備えたものである。

【００４７】

図３は、本発明の実施の形態３に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムをダウンロードする例を示す。

図において、３００は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であり、３０１は制御用マイコン、３０３はあらかじめ暗号化された書き換えプログラムを格納しているメモリ（第１の格納手段）である。半導体集積回路３０８は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）３０２と、復号化回路３０２で復号した書き換えプログラムを格納するための書き換え可能なＲＡＭ（第２の格納手段）３０４と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ３０７の処理を行う演算処理回路（演算処理ユニット）３０５と、ＲＡＭ３０４に格納された書き換えプログラムのうち特定アドレスのみ出力するように制御する制御回路３０６とから構成される。

【００４８】

次に、以上のように構成された半導体集積回路装置３００について、図４のフローチャートを用いて動作を説明する。

暗号化された書き換えプログラムを格納するメモリ３０３からの該書き換えプログラムを復号化回路３０２で復号し（ステップＳ４０１）、該復号化した書き換えプログラムをＲＡＭ３０４に入力する（ステップＳ４０２）。次に、制御回路３０６から、ＲＡＭ３０４に格納されている書き換えプログラムの特定アドレスの読み出しを行い（ステップＳ４０３）、該特定アドレスのプログラムを半導体集積回路３０８外部に読み出してチェックする（ステップＳ４０４）。

【００４９】

以上のような本発明の実施の形態２に係る半導体集積回路装置は、書き換えプログラムをＲＡＭ３０４に格納した後、特定のアドレスのみを半導体集積回路外部に読み出すように制御する制御回路を備え、該読み出された特定アドレスをチェックすることにより、第三者に漏洩したくない機密情報である書き換えプログラムがＲＡＭ３０４に正しく格納されたかどうかを、該書き換えプログラムの機密性を保持しながら判断することができる。

【００５０】

なお、本実施の形態２では特定アドレスのみを読み出し可能としたが、特定ビットのみを半導体集積回路外部に読み出すように制御し、該読み出した特定ビットをチェックしても、書き換えプログラムがＲＡＭに格納されたかどうか判断することができる。

【００５１】

（実施の形態３）

本発明の実施の形態３に係る半導体集積回路装置は、第三者に漏洩したくない機密情報の書き換えプログラムが半導体集積回路内の書き換え可能なＲＡＭに正しく格納されているかを判断するために、該半導体集積回路のＲＡＭに格納した書き換えプログラムの一部を実行するものである。

図５は、本発明の実施の形態３に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムをダウンロードする例を示す。

【００５２】

図において、５００は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であって、５０１は制御用マイコン、５０３は、あらかじめ暗号化された書き換えプログラムを格納しているメモリ（第１の格納手段）である。半導体集積回路５０７は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）５０２と、復号化回路５０２で復号化された書き換えプログラムを格納するための書き換え可能なＲＡＭ（第２の格納手段）５０４と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ５０６の処理を行う演算処理回路（演算処理ユニット）５０５とから構成される。

【００５３】

本実施の形態３において、上記あらかじめ暗号化された書き換えプログラムには、ダウンロード後に該書き換えプログラムの一部を実行するプログラムが含まれているものとする。

【００５４】

次に、以上のように構成された半導体集積回路５００について、図６のフローチャートを用いてその動作を説明する。

メモリ５０３からの暗号化した書き換えプログラムを復号化回路５０２で復号し（ステップＳ６０１）、該復号した書き換えプログラムをＲＡＭ５０４に入力する（ステップＳ６０２）。次に、ＲＡＭ５０４に格納した書き換えプログラムの一部を実行させ（ステップＳ６０３）、正しいか否かが判断されたら、半導体集積回路５０７外部に正しいか否かを通知する信号を出力する（ステップＳ６０４）。

このとき、実行するプログラムの内容を例えばメモリチェックなどのプログラムにし、該メモリチェックを実行させ、そのチェックの結果が得られたならば、ＲＡＭ５０４に正しくプログラムが格納されているかの判断をより確実に行える。

【００５５】

また、図７のように、実行するプログラムの内容を、ＪＵＭＰ命令などを実行して非連続領域のプログラムを実行するプログラムにし、例えば、先頭プログラムでメモリチェックのプログラムのアドレスＸＸにＪＵＭＰする命令を実行するとする。そして、先頭プログラムからメモリチェックのプログラムのアドレスＸＸにＪＵＭＰして、メモリチェックを行うようにすることにより、ＲＡＭ５０４に正しくプログラムが格納されているかの判断をより確実に行える。また、先頭プログラムで最終プログラムのアドレスＹＹにＪＵＭＰする命令を実行するとする。そして先頭プログラムから最終プログラムのアドレスＹＹにＪＵＭＰして、該最終プログラムは、該最終プログラムを実行後にアドレス０１に戻るようなプログラムにして、その結果、プログラムが正しく実行されたことを確認することにより、書き換えプログラムがＲＡＭの最後まで書きこまれているかどうかを判断することができ、特に、暗号化を間違うと後段のデータに影響を及ぼす暗号化方式においては、書き換えプログラムが正しく格納されているかをより一層確実に判断できる。

【００５６】

以上のような本発明の実施の形態３に係る半導体集積回路装置は、書き換えプログラムをＲＡＭ５０４に格納した後、該書き換えプログラムの一部を実行し、正しく実行できた場合に信号を出力することによって、書き換えプログラムがＲ

ＡＭに正しく格納できたかどうかを判断することができる。

【００５７】

また、書き換えプログラムを格納したＲＡＭ５０４から、非連続なプログラム領域を順次実行することにより、書き換えプログラムが最後までＲＡＭに正しく格納されたかを確認することが可能になり、ＲＡＭに格納した書き換えプログラムの正誤チェックを、より確実に行うことができる。

【００５８】

（実施の形態４）

本発明の実施の形態４に係る半導体集積回路装置は、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しく格納されているかを確認するために、半導体集積回路内のＲＡＭに書き換えプログラムを書き込む際に、転送データを監視する転送監視回路を備え、転送されるデータ単位ごとの算術和をとって結果を保持し、チェックサムなどをとるようにしたものである。

【００５９】

図８は、本発明の実施の形態４に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムを半導体集積回路内に格納する例を示す。

図において、８０１は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であって、８０２はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第１の格納手段）であり、８０３は制御用のマイコンである。半導体集積回路８１０は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）８０５と、復号化回路８０５で復号化された書き換えプログラムを格納するためのＲＡＭ（第２の格納手段）８０６と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ８０７の処理を行う演算処理回路（演算処理ユニット）８０８と、復号化回路８０５から転送されるデータ単位ごとの算術和をとる転送監視回路（転送監視手段）８０９とから構成される。

【００６０】

次に、本発明の実施の形態４に係る半導体集積回路装置の動作を説明する。

以上のように構成された半導体集積回路装置８０１において、あらかじめ暗号化されメモリ８０２に格納された書き換えプログラムを、制御用マイコン８０３の制御のもと、復号化回路８０５をとおして復号しながらＲＡＭ８０６に格納する。この時、同時に、データ転送用のデータパスの一部である復号化回路８０５からＲＡＭ８０６への信号線を転送監視回路８０９が常に監視し、転送されるデータ単位ごとの算術和をとって結果を保持していく。そして、メモリ８０２に格納されたデータのうちあらかじめ決められたデータ量の転送が終了した時点で、転送監視回路８０９に保持されている算術和のデータを読み出し、制御用マイコン８０３において、あらかじめ計算しておいた正しく転送がおこなわれたときのデータの算術和と比較し、同じ値であれば転送が正しくおこなわれたと判断し、その後、本来実行すべき処理を行う。もし、この両者の値が異なっていれば、正しく転送がおこなわれなかったと判断し、メモリ８０２に入っているデータを再度転送し直すなど、しかるべき処置を施す。

【００６１】

以上のような本発明の実施の形態４に係る半導体集積回路装置は、書き換えるための書き換えプログラムの転送データを監視し、転送されるデータ単位ごとの算術和をとる転送監視回路を備え、該転送監視回路でとった算術和と、あらかじめ計算しておいた正しく転送が行われたときのデータの算術和とを比較するので、第三者に漏洩したくない機密情報である書き換えプログラムを読み出すことなく、正しくダウンロードされたか否かを判断することができる。

【００６２】

なお、本実施の形態４では、データ転送監視回路を用いてチェックサムをとる例を説明したが、チェックサムの代わりにＣＲＣチェック回路、ＥＣＣチェック回路など、データのあるかたまり単位でビット誤りがあるか否かが判定できるものであれば同様の効果を得ることができ、特にこの監視方式を限定するものではない。

【００６３】

（実施の形態５）

本発明の実施の形態５に係る半導体集積回路装置は、第三者に漏洩したくない

機密情報である書き換えプログラムが、半導体集積回路に正しく格納されているか否かを確認するために、演算処理回路のワークメモリから該演算処理回路を動作させることと、ＲＡＭに格納されたプログラムデータを演算処理回路に入力させることとを可能にし、演算処理回路にて、チェックサムなどをとるようにしたものである。

【００６４】

図９は、本発明の実施の形態５に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムを半導体集積回路内に格納する例を示す。

図において、９０１は、暗号化された書き換えプログラムをもつ半導体集積回路装置であって、９０２はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第１の格納手段）であり、９０３は制御用のマイコンである。半導体集積回路９１５は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）９０５と、復号化回路９０５で復号化された書き換えプログラムを格納するためのＲＡＭ（第２の格納手段）９０６と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ９０７の処理を行う演算処理回路（演算処理ユニット）９０８と、演算処理回路９０８のワークメモリ９１１と、ＲＡＭ９０６、及びワークメモリ９１１のそれぞれを、演算処理回路９０８の命令プログラムを読み込むバス９１３、及びデータを入出力するバス９１４に接続できるように切り替える接続切り替え回路（接続切り替え手段）９１２とから構成されている。また、本実施の形態５において、ＲＡＭ９０６と演算処理回路９０８の命令プログラムを読み込むバス９１３とが接続され、ワークメモリ９１１とデータを入出力するバス９１４とが接続される形態を第１の形態とし、また、ＲＡＭ９０６とデータを入出力するバス９１４とが接続され、ワークメモリ９１１と演算処理回路９０８の命令プログラムを読み込むバス９１３とが接続される形態を第２の形態とし、接続切り替え回路９１２は、上記第１、及び第２の形態のいずれかの形態に切り替えるものである。通常の状態では、上記第１の形態を取るものとし、これらの構成により、演算処理回路９０８は、自分自身の命令プログラムを読み込むバス９１３とデータを読み込むバス９１４とは独立しているいわゆるハーバードアーキテクチュアを取ることができ、より高速に

コンテンツデータ９０７に対するデータ処理が実行できるものである。

【００６５】

次に、本発明の実施の形態５に係る半導体集積回路装置９０１の動作を説明する。

あらかじめ暗号化されメモリ９０２に格納された書き換えプログラムを制御用マイコン９０３の制御のもと、復号化回路９０５をとおして復号しながらＲＡＭ９０６に格納する。その後、演算処理回路９０８の動作を開始する。このとき演算処理回路９０８は、ＲＡＭ９０６の中の書き換えプログラムに組み込まれた実行ステップに応じて動作する。

【００６６】

また、このＲＡＭ９０６に格納された書き換えプログラムの中に、書き換えプログラムがＲＡＭ９０６に正しく格納できたか否かをチェックするプログラム（チェックプログラム）を予め組み込んでおく。本実施の形態５では、データを入出力するバス９１４上のＲＡＭ９０６のデータを読み込み、たとえばチェックサムをとってあらかじめ決められた値と比較することによりＲＡＭ９０６に格納されているデータが正しいことを判定するようなプログラムと、正しいと判断された後に接続切り替え回路９１２を第１の形態に戻すように切り替えるプログラムとの上記２つのプログラムをマシン語データとして組み込んでおき、さらに、該組み込んだマシン語データを直接ワークメモリ９１１に展開するプログラムと、上記マシン語データをワークメモリに展開した後、接続切り替え回路９１２を第２の形態に切り替えるプログラムとを書き換えプログラムの中に予め組み込んでおく。

【００６７】

そして、動作を開始した後、まず、上記予め組み込んでおいたマシン語データを直接ワークメモリ９１１に展開するプログラムにより、上記マシン語データである、上記ＲＡＭ９０６に格納されたプログラムが正しいか否かを判定するための上記２つのプログラムがワークメモリ９１１に展開される。その後、上記接続切り替え回路９１２を第２の形態に切り替えるプログラムによって、接続切り替え回路９１２を第２の形態に切り替える。これにより、ワークメモリ９１１と、

演算処理回路９０８の命令プログラムを読み込むバス９１３とが接続されるため、演算処理回路９０８はワークメモリ９１１に先ほど展開した上記２つのプログラムのうち、データを入出力するバス９１４上のＲＡＭ９０６のデータを読み込み、たとえばチェックサムをとってあらかじめ決められた値と比較することによりＲＡＭ９０６に格納されているデータが正しいことを判定するようなプログラムを実行する。これにより、ＲＡＭ９０６に格納されている書き換えプログラムが正しいと判定されれば、上記ワークメモリ９１１に展開した２つのプログラムの残りのプログラムである、接続切り替え回路９１２を第１の形態に戻すように切り替えるプログラムを実行することによって、接続切り替え回路９１２は第１の形態に切り替えられ、以後本来実行すべきプログラムを実行する。

【００６８】

次に、ＲＡＭ９０６を図１０のような構成にした例を説明する。

このＲＡＭ９０６は、図１０に示すような論理的構成をとるものである。ａ２４００、ａ２４０１、ａ２４０２は、メモリアドレスを示しており、右上がり斜線ハッチをつけたアドレスａ２４００で始まり、アドレスａ２４０１で終わる空間に書き換えプログラムを格納する。また、アドレスａ２４０１で始まり、アドレスａ２４０２で終わる空間には、上記右上がり斜線ハッチをつけたアドレスａ２４００で始まりアドレスａ２４０１で終わる空間に格納されたデータの、たとえばメモリアドレスごとなどのように、あらかじめ決められた単位ごとに対する、たとえばパリティフラグを格納するものとする。

【００６９】

そして、ＲＡＭ９０６に格納する書き換えプログラムの中にあらかじめ組み込んでおくチェックプログラムとして、データを入出力するバス９１４上のＲＡＭ９０６のデータを読み込み、該読み込んだデータの中の１のビットが奇数個あるか偶数個あるかということを数えるいわゆるパリティ演算をおこなうプログラムと、さらに前記読み込んだデータに対応するアドレスａ２４０１からａ２４０２の空間に格納されているパリティフラグの情報を読み込んだ後に、該パリティフラグの情報、及び上記パリティ演算結果の両者を比較してメモリ２４０６に格納された書き換えが正しいか否かを判断するプログラムと、正しいと判断された後

に接続切り替え回路９１２を第１の形態に戻すように切り替えるプログラムとの上記３つのプログラムをマシン語データとして組み込んでおき、さらに、該組み込んだマシン語データを直接ワークメモリ９１１に展開するプログラムと、上記マシン語データをワークメモリに展開した後、接続切り替え回路９１２を第２の形態に切り替えるプログラムとを予め組み込んでおく。

【００７０】

動作を開始した後、まず、上記予め組み込んでおいたマシン語データを直接ワークメモリ９１１に展開するプログラムにより、上記マシン語データである、上記３つのプログラムがワークメモリ９１１に展開される。その後、上記接続切り替え回路９１２を第２の形態に切り替えるプログラムによって、接続切り替え回路９１２を第２の形態に切り替える。これにより、ワークメモリ９１１と演算処理回路９０８の命令プログラムを読み込むバス９１３とが接続されるため、演算処理回路９０８はワークメモリ９１１に先ほど展開した上記３つのプログラムのうち、データを入出力するバス９１４上のメモリのデータを読み込み、該読み込んだデータの中の１のビットが奇数個あるか偶数個あるかということを数えるいわゆるパリティ演算をおこなうプログラムを実行し、次に、前記読み込んだデータに対応するアドレスａ２４０１からａ２４０２の空間に格納されているパリティフラグの情報を読み込んだ後に、該パリティフラグの情報、及び上記パリティ演算結果の両者を比較してＲＡＭ９０６に格納された書き換えプログラムが正しいか否かを判断するプログラムを実行する。これにより正しいと判断されれば、上記ワークメモリ９１１に展開した３つのプログラムの残りのプログラムである、接続切り替え回路９１２を第１の形態に戻すように切り替えるプログラムによって、接続切り替え回路９１２は第１の状態に切り替られ、以後本来実行すべきプログラムを実行する。

【００７１】

このように、ＲＡＭ９０６を上記構成にすることにより、ＲＡＭ９０６に格納した書き換えプログラムが正しく格納されたか否かを確認することができるとともに、書き換えプログラムが正しく格納できていない場合、該正しく格納できていない場所の情報を得ることができる。

【００７２】

なお、ＲＡＭ９０６のアドレスａ２４０１からａ２４０２までの空間に入れるデータは、パリティフラグに限らず、データのあるかたまりで正しいか否かが判定できるものであればよく、現在よく知られているものにＣＲＣチェックやＥＣＣチェックなどがあり、これらを使用しても同様の効果が得られる。

【００７３】

以上のような本発明の実施の形態５に係る半導体集積回路装置は、ＲＡＭ９０６に格納された書き換えプログラムが正しく格納されているかを確認するためのチェックプログラムを演算処理回路のワークメモリ９１１に展開し、接続切り替え回路９１２を切り替えて、ワークメモリ９１１からの命令を可能にし、該ワークメモリ９１１からの命令を受けた演算処理回路にて、チェックサムなどをとることにより、第三者に漏洩したくない機密情報である書き換えプログラムがＲＡＭ９０６に正しく格納されているか否かを、機密性を保持しながら確認することができる。

【００７４】

なお、本発明の実施の形態５に係る半導体集積回路装置では、演算処理回路でチェックサムをとる例を説明したが、チェックサムの代わりにＣＲＣチェック回路、ＥＣＣチェック回路など、データのあるかたまり単位でビットに誤りがあるか否かが判定できるものであれば同様の効果を得ることができる。

【００７５】

（実施の形態６）

本発明の実施の形態６に係る半導体集積回路装置は、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路に正しく格納されたか否かの確認を安定して行うために、ＲＡＭに格納された書き換えプログラムが正しいか否かの確認をするためのチェックプログラムを予めＲＯＭに格納して、該ＲＯＭに格納したチェックプログラムによって、上記書き換えプログラムの確認動作を行うものである。

【００７６】

図１１は、本発明の実施の形態６に係る半導体集積回路装置を示す図であり、

暗号化された書き換えプログラムを半導体集積回路内にダウンロードする例を示す。

図において、１１０１は暗号化された書き換えプログラムをもつ半導体集積回路装置であって、１１０２はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第１の格納手段）であり、半導体集積回路１１１６は、制御用のマイコン１１０３と、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）１１０５と、復号化回路１１０５で復号化した書き換えプログラムを格納するためのＲＡＭ（第２の格納手段）１１０６と、復号化したプログラムの制御手順に従って動作し、コンテンツデータ１１０７の処理を行う演算処理回路（演算処理ユニット）１１０８と、演算処理回路１１０８のワークメモリ１１１１と、ＲＡＭ１１０６、及びワークメモリ１１１１のそれぞれを、演算処理回路１１０８の命令プログラムを読み込むバス１１１３、及びデータを入出力するバス１１１４に接続できるように切り替える接続切り替え回路（接続切り替え手段）１１１２と、演算処理回路１１０８によって実行できるＲＡＭ１１０６に展開された書き換えプログラムが正しいか否かを判定するためのプログラム（チェックプログラム）を格納したＲＯＭ１１１５とから構成され、ＲＯＭ１１１５は、常に演算処理回路１１０８の命令プログラムを読み込むバス１１１３に接続される。また、接続切り替え回路１１１２によって切り替える第１、及び第２の形態は実施の形態５と同様なので説明を省略する。また、実施の形態５と同様、通常の状態では、上記第１の形態を取るものとする。

【００７７】

次に、本発明の実施の形態６に係る半導体集積回路装置の動作を説明する。

まず最初に、あらかじめ暗号化されメモリ１１０２に格納された書き換えプログラムを制御用マイコン１１０３の制御のもと、復号化回路１１０５をとおして復号しながらＲＡＭ１１０６に格納する。その後、演算処理回路１１０８の動作を開始する。この時、切り替え回路１１１２は、第１の形態になるよう接続されているものとする。演算処理回路１１０８は、ＲＡＭ１１０６の中に展開された書き換えプログラムの実行ステップに応じて動作する。この書き換えプログラムの中に、ＲＯＭ１１１５の中にあるデータチェック用のプログラムに制御を移す

ようなプログラムがあり、これを実行する。そして、演算処理回路１１０８の実行プログラムがＲＯＭ１１１５に移った後、接続切り替え回路１１１２を第２の形態になるように切り替える。

【００７８】

これにより、ＲＡＭ１１０６とデータを入出力するバス１１１４とが接続されるため、演算処理回路装置１１０８は、ＲＯＭ１１１５に格納されている、ＲＡＭ１１０６に展開された書き換えプログラムが正しいか否かを判断するプログラムに従い、ＲＡＭ１１０６のデータを読み込み、かつ正しいかどうかの判断をする。

正しいと判断されれば、ＲＯＭ１１１５に組み込まれている接続切り替え回路１１１２を第１の形態に戻すように切り替えるプログラムによって、接続切り替え回路２５１２は第１の状態に切り替られ、以後本来実行すべきプログラムを実行する。

【００７９】

なお、ＲＡＭ１１０６に格納されている書き換えプログラムが正しいか否かを確認する方法は、ＲＯＭ１１１５に実装されている方式によるが、この方式には、たとえばチェックサムなどが用いられる。しかしながら、必ずしも方式を限定するものではなく、データのある決められた固まり単位で正しいことが判定できればよいことは言うまでもない。

【００８０】

次に、ＲＡＭ１１０６を図１２のような構成にした場合について説明する。

図１２は、本発明の実施の形態６に係る半導体集積回路装置のＲＡＭ１１０６の例を示したものである。

図において、ａ２６００、ａ２６０１、ａ２６０２、ａ２６０３、ａ２６０４は、メモリアドレスを示しており、ａ２６００はＲＡＭ１１０６におけるスタートアドレスを示し、ａ２６０４はエンドアドレスを示す。また、右上がり斜線ハッチをつけて示すように、ａ２６０１はＲＡＭ１１０６の全容量のちょうど半分に位置する場所のアドレスを示している。また、右下がり斜線をつけて示すように、ａ２６０２はアドレスａ２６０１とエンドアドレスａ２６０４とであらわさ

れた容量のちょうど半分に位置する場所のアドレスを示す。同様に、ａ２６０３はアドレスａ２６０２とエンドアドレスａ２６０４とであらわされる容量のちょうど半分に位置するアドレスを示している。

【００８１】

以上のようなＲＡＭ１１０６を用いた半導体集積回路装置１１０１の動作について説明する。

まず最初に、ＲＡＭ１１０６のアドレスａ２６００からａ２６０１までの部分にメモリ１１０２から復号化回路１１０５を通してデータをダウンロードする。そのあと、アドレスａ２６０１からａ２６０４までの領域にも、ＲＡＭ１１０２に格納されている先に展開したアドレスａ２６００からａ２６０１までのデータと全く同じデータを、これも同様に復号化しながらダウンロードする。この後、接続切り替え回路１１１２を切り替えてＲＡＭ１１０６のデータを読み出す。この読み出し時に、アドレスａ２６００からとアドレスａ２６０１からとのそれぞれ等距離にあるものを順次アクセスし、得られたデータのビットごとの排他的論理和を取る。暗号が正しく解け、データパスに異常がなく、かつ、ＲＡＭ１１０６の格納域ビットに異常がなければ、この排他的論理和の結果は、あるデータと同じデータとの排他的論理和となるため、０になる。したがって、この手順を準次繰り返し、各排他的論理和が０であることを確かめれば、メモリ１１０２から復号化回路１１０５を通してＲＡＭ１１０６に正しく展開できているという判断ができる。上記手順を残り領域の１／２ずつ繰り返し実行することで、ＲＡＭ１１０６には、演算処理回路１１０８のプログラムが復号化されてダウンロードされ、同時に、そのデータ内容が期待どおりであることが確かめられる。

【００８２】

このように、ＲＡＭ１１０６を上記構成にすることにより、何らかの不具合のために、上記手順の排他的論理和が０とならない場合には、ＲＡＭ１１０６に格納されているデータに不具合があると判断できるとともに、不具合発生アドレスも知ることができる。

なお、メモリ１１０２からＲＡＭ１１０６に展開するデータ量は、ＲＡＭ１１０６の書き換えプログラムが格納されていない領域の１／２以下ずつであればよ

いが、排他的論理和をとる上記方法においては、１／２が読み出し可能な最大データ量であるので、１／２とすることで書き込み効率を大きくとれる。

【００８３】

また、本実施の形態６において、このように構成されたＲＡＭ１１０６を用いて、データチェックプログラムＲＯＭ１１１５に格納されたプログラムに基づいてデータチェックを行う例を説明したが、データチェックプログラムＲＯＭ１１１５がない場合でも、実施の形態５のように、ダウンロードするプログラムに予めデータチェックプログラムを組み込むようにすることにより同様の効果を得ることができる。

【００８４】

次に、メモリ１１０２の構成を図１３のような構成にした場合について説明する。

図１３は、本発明の実施の形態６に係る半導体集積回路装置におけるメモリ１１０２の例を示したものである。

【００８５】

図において、ａ２７１０、ａ２７１１、ａ２７１２、ａ２７１３、ａ２７１４、ａ２７１５、ａ２７１６、ａ２７１７は、メモリ１１０２におけるアドレスを示している。アドレスａ２７１０は、メモリ１１０２のスタートアドレスを示し、アドレスａ２７１７は、メモリ１１０２のエンドアドレスを示す。また、アドレスａ２７１０とアドレスａ２７１１に囲まれた空間には、図１２で示したＲＡＭ１１０６のアドレスａ２６００からａ２６０１に入るべきデータを暗号化して格納する。便宜上これを「データＡ」と呼ぶ。また、アドレスａ２７１１とアドレスａ２７１２に囲まれた空間には、復号化回路１１０５によって復号化するとＲＡＭ１１０６のアドレスａ２６００からａ２６０１に入るべきデータ、即ち「データＡ」を各ビットごとに反転したものが得られるようなデータが格納される。これを便宜上「データＡ´」と呼ぶ。同様に、アドレスａ２７１２とアドレスａ２７１３に囲まれた空間には、ＲＡＭ１１０６のアドレスａ２６０１からａ２６０２に入るべきデータを暗号化したものを格納し、アドレスａ２７１３とアドレスａ２７１４に囲まれた空間には、復号化回路１１０５によって復号化すると

ＲＡＭ１１０６のアドレスａ２６０１からａ２６０２に入るべきデータを各ビットごとに反転したものが得られるようなデータが格納される。これらを便宜上それぞれ、「データＢ」「データＢ´」と呼ぶ。「データＣ」及び「データＣ´」も同様の対応である。このような手順を繰り返し、ＲＡＭ１１０６に格納すべき全てのプログラム及びその反転データを上記手順に従って、暗号化してメモリ１１０２に格納する。

【００８６】

以上のように構成されたメモリ１１０２、及びＲＡＭ１１０６を使った半導体集積回路装置１１０１の動作について説明する。

まず、ＲＡＭ１１０６のアドレスａ２６００からａ２６０１までの部分にメモリ１１０２から復号化回路１１０５を通して「データＡ」をダウンロードする。そのあと、上記手順にて述べたメモリ１１０２に格納されている今ダウンロードしたデータの反転データを暗号化したものである「データＡ´」を、これも同様に復号化しながらダウンロードする。この後、接続切り替え回路１１１２を切り替えてＲＡＭ１１０６のデータを読み出す。この読み出し時に、アドレスａ２６００からとアドレスａ２６０１からとのそれぞれ等距離にあるものを順次アクセスし、得られたデータのビットごとの論理積を取る。暗号が正しく解け、データパスに異常がなく、かつ、ＲＡＭ１１０６の格納域ビットに異常がなければ、この論理積の結果は、あるデータとその反転データとの論理積となるため、０になる。したがって、この手順を順次繰り返し、各論理積が０であることをたしかめれば、メモリ１１０２から復号化回路１１０５を通してＲＡＭ１１０６に正しく展開できているということになる。メモリ１１０２には、ＲＡＭ１１０６の各手順における残りの領域の１／２ずつのデータとその反転データが暗号化されて「データＢ」「データＢ´」「データＣ」「データＣ´」などのように対になって必要な量だけ格納されており、上記手順を残り領域の１／２づつデータがなくなるまで繰り返し実行することで、ＲＡＭ１１０６には、演算処理回路１１０８のプログラムが復号化されてダウンロードされ、同時に、そのデータ内容が期待どおりであることが確かめられる。

【００８７】

これにより、もしも何らかの不具合のために、上記手順の論理積が０とならない場合に、ＲＡＭ１１０６に格納されているデータに不具合があると判断できるとともに、不具合発生アドレスも知ることができる。また、何らかの理由により、復号化回路１１０５に不具合がありＲＡＭ１１０６への出力が固定値になっていても、ＲＡＭ２５０６に格納されているデータを上記手順で論理積をとれば、あるデータと同じデータの論理積であるため、０にはならない。このことで、正しくデータが格納されてはいないと判断できる。

【００８８】

なお、メモリ１１０２からＲＡＭ１１０６に展開するデータ量は、該ＲＡＭ１１０６の残り領域の１／２以下ずつであってもよいが、論理積をとる上記方法においてはＲＡＭ１１０６の残り領域の１／２が読み出し可能な最大データ量であるので、１／２とすることで書き込み効率を大きくとれる。

【００８９】

また、本実施の形態６において、このように構成されたメモリ１１０２を用いて、データチェックプログラムＲＯＭ１１１５に格納されたプログラムに基づいてデータチェックを行う例を説明したが、データチェックプログラムＲＯＭ１１１５がない場合でも、実施の形態５のように、ダウンロードする書き換えプログラムに予めチェックプログラムを組み込むようにすることにより同様の効果を得ることができる。

【００９０】

以上のような本発明の実施の形態６に係る半導体集積回路装置は、ＲＡＭ１１０６に格納されている書き換えプログラムが正しく格納されているか否かを確認するためのチェックプログラムをＲＯＭ化したメモリ１１１５に格納したので、チェックプログラムの転送や、展開に誤りが発生しても、ＲＡＭ１１０６に格納された書き換えプログラムが正しく格納できたか否かの確認を、容易に、かつ、安定して行うことができる。

【００９１】

また、ＲＡＭ１１０６の書き換えプログラムが格納されていない領域を２分割した各々の領域に、該書き換えプログラムが格納されていない領域の１／２に相

当するプログラムデータと、該１／２の領域に読み出したプログラムデータと同じデータとを順次読み出し、該読み出したそれぞれのデータから排他的論理和をとる手順を繰り返し行うようにしたので、ＲＡＭ１１０６に格納された書き換えプログラムが正しく格納されたかを確認することができるとともに、書き換えプログラムがＲＡＭ１１０６に正しく格納できていない場合に、ＲＡＭ１１０６における正しく格納できていない場所の情報を得ることができる。

【００９２】

また、ＲＡＭ１１０６の書き換えプログラムが格納されていない領域を２分割した各々の領域に、該書き換えプログラムが格納されていない領域の１／２に相当するプログラムデータと、該１／２の領域に読み出したプログラムデータを反転したデータとを順次読み出し、該読み出したそれぞれのデータから論理積をとる手順を繰り返し行うようにしたので、ＲＡＭ１１０６に格納された書き換えプログラムが正しく格納されたかを確認することができるとともに、何らかの理由により復号化回路１１０５の不具合でＲＡＭ１１０６への出力が固定値になり、排他的論理和をとってもデータが一致し、上記第２の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、ＲＡＭ１１０６に格納したプログラムの正誤を正しく判別できる。

【００９３】

なお、本発明の実施の形態１～６に係る半導体集積回路装置では、予め暗号化した書き換えプログラムを、半導体集積回路内にダウンロードする例を説明したが、暗号化されていない書き換えプログラムを半導体集積回路内にダウンロードしても同様の効果が得られるのはいうまでもない。

【００９４】

（実施の形態７）

本発明の実施の形態７に係る半導体集積回路装置は、予め暗号化された書き換えプログラムをメモリに格納した半導体集積回路装置において、第三者に漏洩したくない機密情報である書き換えプログラムが正しく格納されたか否かを、該書き換えプログラムの機密性を保持しながら確認するために、上記暗号化された書き換えプログラムを復号してＲＡＭに格納した後、該書き換えプログラムを再度

暗号化し、該再度暗号化したプログラムデータと、上記予め暗号化されたプログラムデータとを比較するようにしたものである。

【００９５】

図１４は、本発明の実施の形態７に係る半導体集積回路装置の構成を示す図である。

図において、１４０１は暗号化された書き換えプログラムをもつ半導体集積回路装置であり、１４０２はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第１の格納手段）であり、１４０３は制御用のマイコンである。半導体集積回路１４１１は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）１４０５と、復号化回路で復号された書き換えプログラムを格納するためのＲＡＭ（第２の格納手段）１４０６と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ１４０７の処理を行う演算処理回路（演算処理ユニット）１４０８と、上記ＲＡＭ１４０６に転送されたデータを再度暗号化する暗号化回路（暗号化手段）１４１０とから構成される。

【００９６】

次に、以上のように構成された半導体集積回路装置１４０１の動作を説明する。

まず、あらかじめ暗号化されメモリ１４０２に格納された書き換えプログラムを制御用マイコン１４０３の制御のもと、復号化回路１４０５をとおして復号しながらＲＡＭ１４０６に格納する。そして、メモリ１４０２に格納されたデータのうち、あらかじめ決められたデータ量の転送が終了した時点で、今度は、制御用マイコン１４０３の制御のもと、今復号化してメモリ１４０６に格納した書き換えプログラムを読み出し、暗号化回路１４１０を通して再度暗号化し、該再度暗号化したプログラムデータとメモリ１４０２に格納されている予め暗号化したプログラムデータとを比較する。この両者のデータが一致すれば、最初にメモリ１４０２から読み出し、復号化回路１４０５にて復号化し、ＲＡＭ１４０６に格納した書き換えプログラムが、正しいと判断できる。

【００９７】

以上のような、本発明の実施の形態７に係る半導体集積回路装置は、予め暗号化したプログラムを半導体集積回路１４１１にダウンロードする半導体集積回路装置において、暗号化した書き換えプログラムを復号化し、ＲＡＭ１４０６に格納した後、暗号化回路１４１０で再度暗号化し、予め暗号化した書き換えプログラムと再度暗号化した書き換えプログラムとを比較するようにしたので、第三者に漏洩したくない機密情報の書き換えプログラムをそのまま外部に読み出すことなく、ＲＡＭ１４０６に格納した書き換えプログラムが正しく格納できたか否かを確認することができる。

【００９８】

（実施の形態８）

本発明の実施の形態８に係る半導体集積回路装置は、ＲＡＭに格納した書き換えプログラムが正しくないと判定された場合、該書き換えプログラムの修正箇所を検出して書き換えプログラムを修正可能にしたものである。

以下、本発明の実施の形態８に係る半導体集積回路装置を、図１５、図１６、及び図１７を用いて説明する。

【００９９】

図１５は、本発明の実施の形態８に係る半導体集積回路装置の構成を示した図であり、実施の形態７で説明した半導体集積回路装置において、ＲＡＭに格納されたプログラムが正しくないと判断された場合、プログラムを修正可能とする例を示したものである。

【０１００】

図において、１５００は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であって、１５０３はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第１の格納手段）であり、１５０１は制御用のマイコンである。半導体集積回路１５０９は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）１５０２と、復号化回路１５０２で復号された書き換えプログラムを格納するためのＲＡＭ（第２の格納手段）１５０４と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ１５０８の処理を行う演算処理回路（演算処理ユニット）１５０５と、

ＲＡＭ１５０４に格納された書き換えプログラムを再度暗号化する暗号化回路１５０６とから構成される。ここまでの構成は図１４の半導体集積回路装置１４０１と同じであるが、半導体集積回路装置１５００においては、暗号化回路１５０６の出力Ｓ１５０６とあらかじめ暗号化された書き換えプログラムが格納されているメモリ１５０３の出力Ｓ１５０３とを比較し、ＲＡＭ１５０４に正しく格納されなかった場所を検出する比較器１５０７を備えている。

【０１０１】

以上のように構成された半導体集積回路装置１５００について、以下にその動作を説明する。図１６は、実施の形態８に係る半導体回路１５００の動作フローを示す。

まず、暗号化した書き換えプログラムを復号化回路１５０２で復号し（ステップＳ１６０１）、制御用マイコン１５０１にしたがい、復号化した書き換えプログラムをＲＡＭ１５０４に入力する（ステップＳ１６０２）。ステップＳ１６０２でＲＡＭ１５０４に入力した書き換えプログラムを暗号化回路１５０６で再度、暗号化し（ステップＳ１６０３）、ステップＳ１６０３で暗号化した書き換えプログラムとメモリ１５０３に保持している書き換えプログラムとを比較する（ステップＳ１６０４）。ステップＳ１６０４でのチェックで正しくない場合、制御用マイコン１５０１に従って、正しくない部分のＲＡＭのビットを使用しないように書き換えプログラムを修正する（ステップＳ１６０５）。そして、ステップＳ１６０５で修正したプログラムを復号化し（ステップＳ１６０６）、該復号化したプログラムをＲＡＭ１５０４に入力する（ステップＳ１６０７）。

【０１０２】

また、ステップＳ１６０５の書き換えプログラム修正の動作は、例えば、図１７のように、ＲＡＭ１５０４に格納された書き換えプログラムの正しくない部分が、例えばマシン語単位などあらかじめ決められた単位のアドレスＸＸからアドレスＸＸ´とすると、アドレスＸＸからアドレスＸＸ´に格納されるべきデータを修正プログラムとしてアドレスＹＹからアドレスＹＹ´に格納するようにする。このとき、修正プログラムに、アドレスＸＸまで読み出したときにアドレスＹＹにＪＵＭＰする命令プログラムと、次にアドレスＹＹ´まで読み出したときに

アドレスＸＸ´にＪＵＭＰする命令プログラムとを組み込んでおくことにより、ＲＡＭ１５０４に格納されたプログラムの読み出しを正常に行うことができる。

【０１０３】

これにより、上記方法によると、修正プログラムをＲＡＭ１５０４に入力した後、読み出してチェックすることによりＲＡＭ１５０４内の欠陥のあるビットを使わないようにできるため、ＲＡＭの有効活用ができる。

【０１０４】

なお、本実施の形態８では、予め暗号化した書き換えプログラムを格納するメモリ１５０３からの出力Ｓ１５０３と復号した書き換えプログラムを再度暗号化する暗号化回路１５０６からの出力Ｓ１５０６とを比較した結果から、ＲＡＭ１５０４に正しく格納できなかった場所を検出して、書き換えプログラムを修正したが、上述した書き換えプログラムの修正は、ＲＡＭの欠陥位置を検出できれば可能であるので、実施の形態６で説明したメモリ、及びＲＡＭの構成により読み出したデータの排他的論理和、及び論理積をとってデータをチェックする例においても適用可能である。

【０１０５】

以上のような、実施の形態８に係る半導体集積回路装置は、書き換えプログラムがＲＡＭに正しく格納されたか否かを確認した結果、ＲＡＭに正しく格納されなかった場合に、正しく書き込めていないＲＡＭのビットを使用しないように書き換えプログラムを修正して、ＲＡＭにダウンロードするので、ＲＡＭの一部のビットが正しく生成できていなくても、その他の部分に書き込んで、書き換えプログラムを正しく動作させることができ、ＲＡＭを有効に活用することができる。

【０１０６】

なお、本発明の実施の形態１～８の半導体集積回路装置では、書き換えプログラムをメモリ（第１の格納手段）に格納して、半導体集積回路内にダウンロードしたが、半導体集積回路装置外部に書き換えプログラムを保持し、例えば、インターネット等の通信手段を用いて、半導体集積回路内にダウンロードしても同様の効果を得ることができるのはいうまでもない。

【０１０７】

【発明の効果】

以上のような、本発明の請求項１に係る半導体集積回路装置によれば、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記第２の格納手段は、該半導体集積回路外部から読出しが可能な外部読出し可能領域と、読出しが不可能な外部読出し不可能領域とを有するものであり、上記第２の格納手段の外部読出し可能領域に任意のデータを入力格納したのち、該データを該半導体集積回路の外部に読出して、該任意のデータが上記入力した通りのデータであるかを確認し、そののち、上記第１の格納手段からの上記書き換えプログラムを、上記第２の格納手段の外部読出し不可能領域に格納するようにしたので、例えばダミーデータなどを、上記第２の格納手段の読み出し可能な領域に書き込んで、該書き込んだダミーデータを読み出してチェックをすることにより、半導体集積回路内に正しく上記書き換えプログラムが格納されたかどうかを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【０１０８】

また、本発明の請求項２に係る半導体集積回路装置によれば、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記第２の格納手段に格納された上記書き換えプログラムの特定部分のみを読み出すように制御する制御回路を備えたものとしたので、上記第２の格納手段に格納された特定部分のみを読み出して、該特定部分を検証することにより、上記

書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【０１０９】

また、本発明の請求項３に係る半導体集積回路装置によれば、請求項２に記載の半導体集積回路装置において、上記制御回路は、上記第２の格納手段の特定のアドレスにある書き換えプログラムのみを読み出すように制御するもの、としたので、上記第２の格納手段の特定のアドレスのみを読み出して、該特定のアドレスのデータを検証することにより、上記書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【０１１０】

また、本発明の請求項４に係る半導体集積回路装置によれば、請求項２に記載の半導体集積回路装置において、上記制御回路は、上記第２の格納手段に格納した書き換えプログラムの特定のビットのみを読み出すように制御するものとしたので、上記第２の格納手段の特定のビットのみを読み出して、該特定のビットのみを検証することにより、上記書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【０１１１】

また、本発明の請求項５に係る半導体集積回路装置によれば、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記書き換えプログラムは、書き換え後に該プログラムの一部を実行するプログラムを含んだものであり、上記第２の格納手段に格納した上記書き換えプログラムの一部を実行するので、第三者に漏洩したくない機密情報である書き換えプ

ログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【０１１２】

また、本発明の請求項６に係る半導体集積回路装置によれば、請求項５に記載の半導体集積回路装置において、上記実行する書き換えプログラムの一部は、非連続なプログラム領域を順次実行するものであるので、例えば、上記第２の格納手段に格納した書き換えプログラムの先頭プログラムと最終プログラムとを実行した場合、該書き換えプログラムが最後まで正しく格納できたかを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【０１１３】

また、本発明の請求項７に係る半導体集積回路装置によれば、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記半導体集積回路内に、上記第１の格納手段から上記第２の格納手段に転送される上記書き換えプログラムを監視する転送監視手段を備えたものとしたので、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【０１１４】

また、本発明の請求項８に係る半導体集積回路装置によれば、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記書き換えプログラムは、プログラムの正誤の判定を行うチェックプログラ

ムが含まれたものであり、上記半導体集積回路内に、上記演算処理ユニットのワークメモリと、上記第２の格納手段または上記ワークメモリと、上記演算処理ユニットのプログラム入力またはデータ入力との接続を切り替える接続切り替え手段とを備え、上記第２の格納手段に格納された上記書き換えプログラムから抽出した上記チェックプログラムを上記ワークメモリに格納し、該ワークメモリに格納したチェックプログラムにより、上記演算処理ユニットを動作させ、上記書き換えプログラムの正誤チェックを行うので、接続切り換え手段にて演算処理ユニットのプログラム入力あるいはデータ入力を切り替えて、上記書き換えプログラムのデータを取り込んで、例えば該書き換えプログラムのデータのチェックサムなどをとって、予め決めておいた値と比較することが可能となり、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【０１１５】

また、本発明の請求項９に記載の半導体集積回路装置によれば、請求項８に記載の半導体集積回路装置において、上記第２の格納手段は、上記書き換えプログラムを格納するとともに、該書き換えプログラムのうち、ある決められたかたまりから所定の法則に従い一意に得られるデータを格納するものとしたので、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第２の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる効果がある。

【０１１６】

また、本発明の請求項１０に係る半導体集積回路装置によれば、請求項９に記載の半導体集積回路装置において、上記一意に得られるデータを、上記プログラムの正誤チェックをするためのチェックコードとして使用するので、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第２の格納手段に正しく格納できなかった場合

、正しく格納できていない場所の情報を得ることができる効果がある。

【０１１７】

また、本発明の請求項１１に係る半導体集積回路装置によれば、請求項８に記載の半導体集積回路装置において、上記第２の格納手段は、その構成を、上記書き換えプログラムが格納されていない領域を順次２分割した構成とし、該２分割した各々の領域に同じプログラムデータを格納するものであり、上記チェックプログラムは、上記２分割した両領域の各々に格納された同じプログラムデータを比較して正誤を判定するプログラムと、前回の判定結果が正しいと判定されたときに、前回２分割した領域の1方の領域を、プログラムが格納されていない領域としてさらに２分割し、該分割した領域の各々に同じプログラムデータを格納する動作を繰り返すプログラムとを有し、上記第２の格納手段に格納すべきプログラムすべてを順次格納するので、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第２の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる効果がある。

【０１１８】

また、本発明の請求項１２に係る半導体集積回路装置によれば、請求項１１に記載の半導体集積回路装置において、上記第２の格納手段は、該第２の格納手段の上記書き換えプログラムが格納されていない領域を順次２分割した各々の領域に、上記書き換えプログラムデータと、該プログラムデータから所定の法則に従い一意に得られるデータとを格納するものとしたので、例えば、第２の格納手段の前段に復号化回路を備えて、該復号化回路の不具合により出力が固定値になり、排他的論理和をとってもデータが一致し、上記第２の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、第２の格納手段に格納した書き換えプログラムの誤りを容易に見つけ出すことができる効果がある。

【０１１９】

また、本発明の請求項１３に係る半導体集積回路装置によれば、請求項１２に

記載の半導体集積回路装置において、上記一意に得られるデータが、該プログラムデータの反転データであるので、例えば、第２の格納手段の前段に復号化回路を備えて、該復号化回路の不具合により出力が固定値になり、排他的論理和をとってもデータが一致し、上記第２の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、第２の格納手段に格納した書き換えプログラムの誤りを容易に見つけ出すことができる効果がある。

【０１２０】

また、本発明の請求項１４に係る半導体集積回路装置によれば、請求項８ないし１３のいずれかに記載の半導体集積回路装置において、上記チェックプログラムを予め格納したＲＯＭ（Read Only Memory）を備え、上記ＲＯＭにより上記演算処理ユニットを動作させて、上記書き換えプログラムの正誤チェックを行うので、上記チェックプログラムの転送誤り等により、チェックプログラムが機能しなくなるのを防ぎ、上記第２の格納手段に上記書き換えプログラムが正しく格納できたか否かを確認するチェックプログラムを安定的に提供することができる効果がある。

【０１２１】

また、本発明の請求項１５に係る半導体集積回路装置によれば、請求項１ないし１４のいずれかに記載の半導体集積回路装置において、上記半導体集積回路内に、暗号化された書き換えプログラムを復号する復号化手段を備え、上記第１の格納手段に格納された書き換えプログラムが予め暗号化されている場合、上記復号化手段は、該暗号化プログラムを復号化し、上記第２の格納手段に復号化した上記書き換えプログラムを格納するので、第三者に漏洩したくない機密情報であり、また、予め暗号化されている書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【０１２２】

また、本発明の請求項１６に係る半導体集積回路装置によれば、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第２の格納手段を半導体集積回路内に有し、該第２

の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である、予め暗号化された書き換えプログラムを格納する第１の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記半導体集積回路内に、上記第１の格納手段からの上記暗号化された書き換えプログラムを復号化し、該復号化した書き換えプログラムを上記第２の格納手段に転送する復号化手段と、上記第２の格納手段に格納した書き換えプログラムを再度暗号化する暗号化手段とを備え、上記暗号化手段で暗号化された書き換えプログラムと上記第１の格納手段に保持している暗号化されたプログラムとを比較するので、第三者に漏洩したくない機密情報であり、また、予め暗号化されている書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【０１２３】

また、本発明の請求項１７に係る半導体集積回路装置によれば、請求項１１ないし１３、及び１６のいずれかに記載の半導体集積回路装置において、上記第２の格納手段にデータが正しく格納されていない場合、不良箇所を検出し、上記第１の格納手段に保持した書き換えプログラムを修正可能としたので、第２の格納手段において、正しく格納できなかった箇所を使用しないように書き換えプログラムを修正して書き込むので、メモリを有効に活用することができる効果がある。

【０１２４】

また、本発明の請求項１８に係る半導体集積回路装置によれば、請求項１ないし１７のいずれかに記載の半導体集積回路装置において、当該半導体集積回路装置外部に保持した書き換えプログラムを、上記半導体集積回路内にダウンロード可能としたので、書き換えプログラムを半導体集積回路装置外部に有する場合においても、ネットワーク等の通信手段を用いてダウンロードでき、第三者に漏洩したくない機密情報である書き換えプログラムが正しく格納できたか否かを、機密性を保持しながら確認することができる効果がある。

【図面の簡単な説明】

【図１】

本発明の実施の形態１における半導体集積回路装置を示す図

【図２】

本発明の実施の形態１における半導体集積回路装置の動作を示すフローチャート

【図３】

本発明の実施の形態２における半導体集積回路装置を示す図

【図４】

本発明の実施の形態２における半導体集積回路装置の動作を示すフローチャート

【図５】

本発明の実施の形態３における半導体集積回路装置を示す図

【図６】

本発明の実施の形態３における半導体集積回路装置を示す図

【図７】

本発明の実施の形態３における半導体集積回路の実行プログラムの一例を示す図

【図８】

本発明の実施の形態４における半導体集積回路装置を示す図

【図９】

本発明の実施の形態５における半導体集積回路装置を示すブロック構成図

【図１０】

本発明の実施の形態５における半導体集積回路装置のＲＡＭ（第２の格納手段）の構成の一例を示す構成図

【図１１】

本発明の実施の形態６における半導体集積回路装置を示すブロック構成図

【図１２】

本発明の実施の形態６における半導体集積回路装置のＲＡＭ（第２の格納手段）１１０６の構成の一例を示す図

【図１３】

本発明の実施の形態６におけるメモリ１１０２内のデータ配置を示す概念図

【図１４】

本発明の実施の形態７における半導体集積回路装置を示すブロック構成図

【図１５】

本発明の実施の形態８における半導体集積回路装置を示すブロック構成図

【図１６】

本発明の実施の形態８における半導体集積回路装置の動作を示すフローチャート

【図１７】

本発明の実施の形態８における半導体集積回路装置のプログラムの修正を行う一例を示した図

【符号の説明】

１００、３００、５００、８０１、９０１、１１０１、１４０１、１５００　半導体集積回路装置

１０９、３０８、５０７、８１０、９１５、１１１６、１４１１、１５０９　半導体集積回路

１０１、３０３、５０３、８０２、９０２、１１０２、１４０２、１５０３　暗号化されたプログラムを格納しているメモリ（第１の格納手段）

１０５、３０１、５０１、８０３、９０３、１１０３、１４０３、１５０１　制御用のマイコン

１０２、３０２、５０２、８０５、９０６、１１０５、１４０５、１５０２　復号化回路（復号化手段）

１０８、３０４、５０４、８０６、９０６、１１０６、１４０６、１５０４　プログラムを格納するＲＡＭ（第２の格納手段）

１０３　プログラムを格納するＲＡＭ１０８の外部読出し可能領域

１０４　プログラムを格納するＲＡＭ１０８の外部読出し不可能領域

１０６、３０５、５０５、８０８、９０８、１１０８、１４０８、１５０５　演算処理回路（演算処理ユニット）

１０７、３０７、５０６、８０７、９０７、１１０７、１４０７、１５０８　コンテンツデータ

３０６　制御回路

８０９　転送監視回路（転送監視手段）

９１１、１１１１、　ワークメモリ

９１２、１１１２　接続切り替え回路

９１３、１１１３　命令プログラムを読み込むバス

９１４、１１１４　データを入出力するバス

１１１５　データチェックプログラムＲＯＭ

１５０６　暗号化回路（暗号化手段）

Ｓ１５０３　暗号化されたプログラムを格納しているメモリ１５０３の出力信号

Ｓ１５０６　暗号化回路１５０６の出力信号

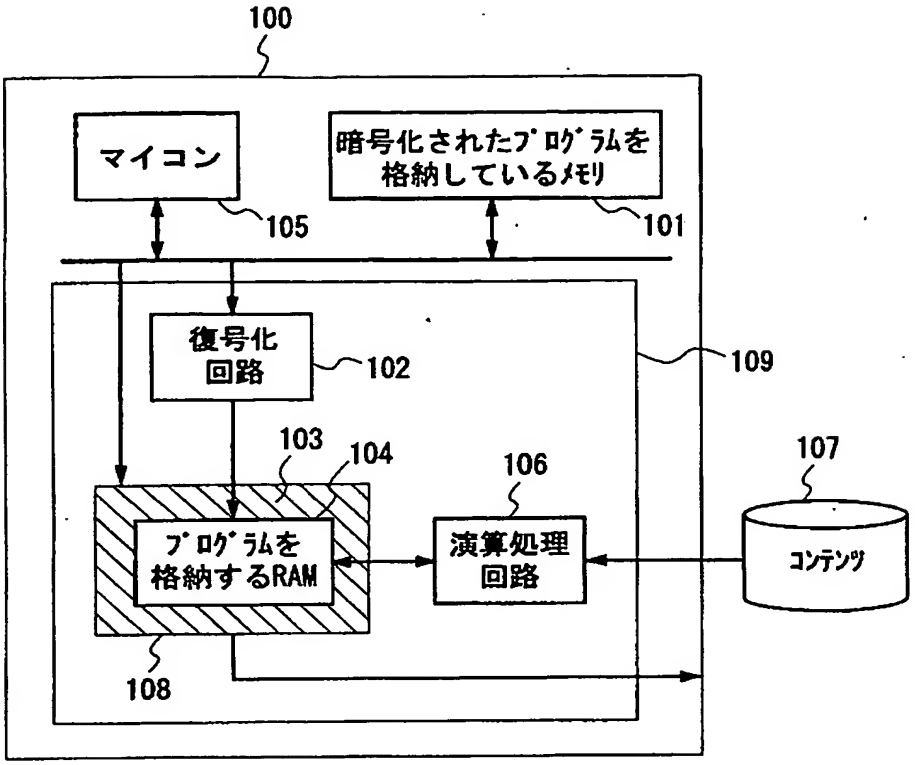
ａ２４００～ａ２４０２　プログラムを格納するＲＡＭ９０６のアドレス

ａ２６００～ａ２６０４　プログラムを格納するＲＡＭ１１０６のアドレス

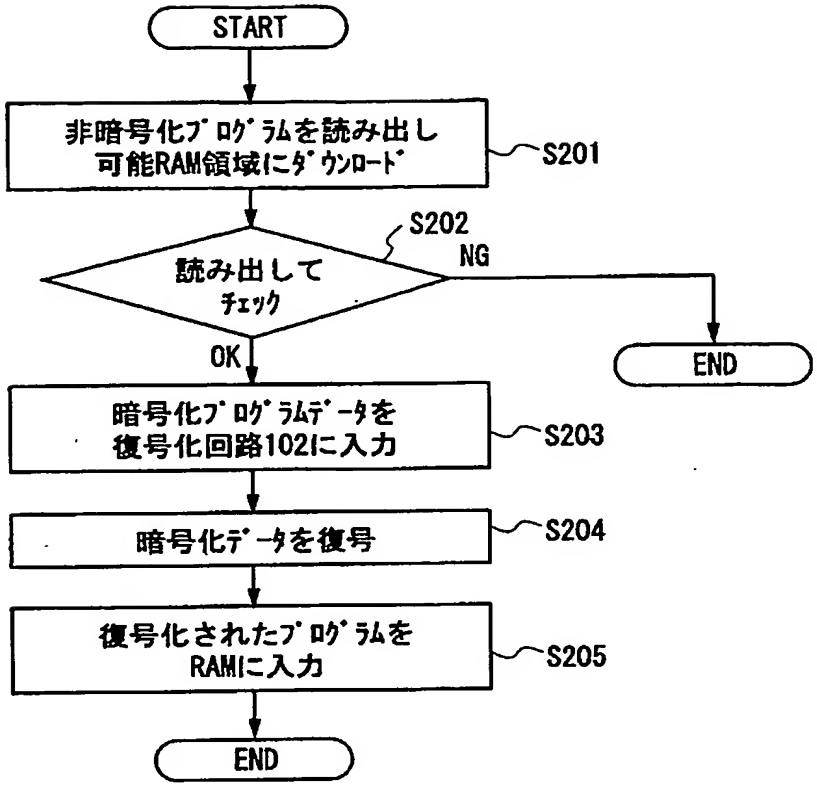
ａ２７１０～ａ２７１７　暗号化されたプログラムを格納するメモリ１１０２のアドレス

【書類名】　図面

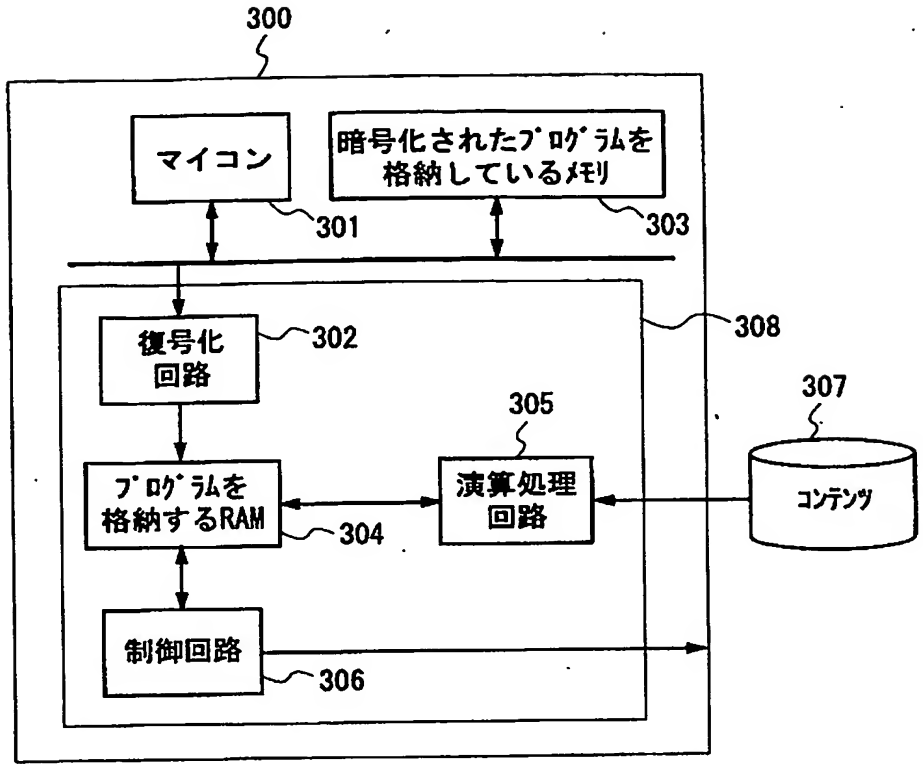
【図１】


100
マイコン
105
暗号化されたﾌﾟﾛｸﾞﾗﾑを
格納しているﾒﾓﾘ
101
復号化
回路
102
109
103
104
106
107
ﾌﾟﾛｸﾞﾗﾑを
格納するRAM
演算処理
回路
ｺﾝﾃﾝﾂ
108

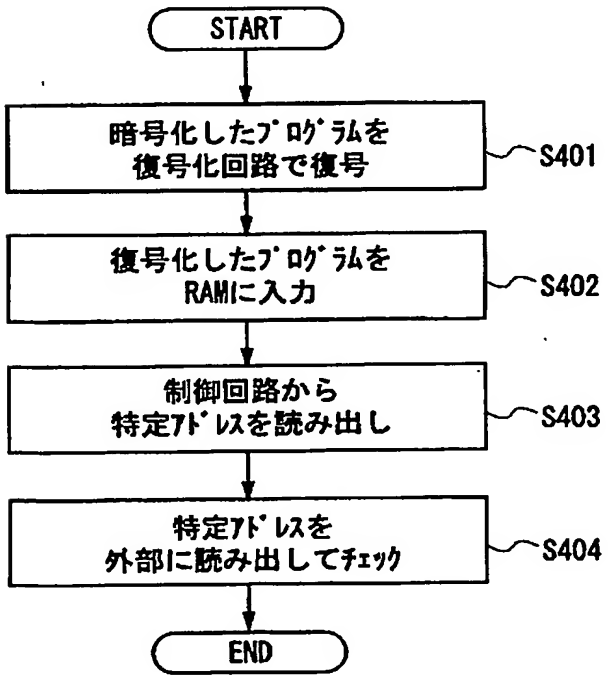
【図２】


START
非暗号化ﾌﾟﾛｸﾞﾗﾑを読み出し
可能RAM領域にﾀﾞｳﾝﾛｰﾄﾞ
S201
S202
読み出して
ﾁｪｯｸ
NG
END
OK
暗号化ﾌﾟﾛｸﾞﾗﾑﾃﾞｰﾀを
復号化回路102に入力
S203
暗号化ﾃﾞｰﾀを復号
S204
復号化されたﾌﾟﾛｸﾞﾗﾑを
RAMに入力
S205
END

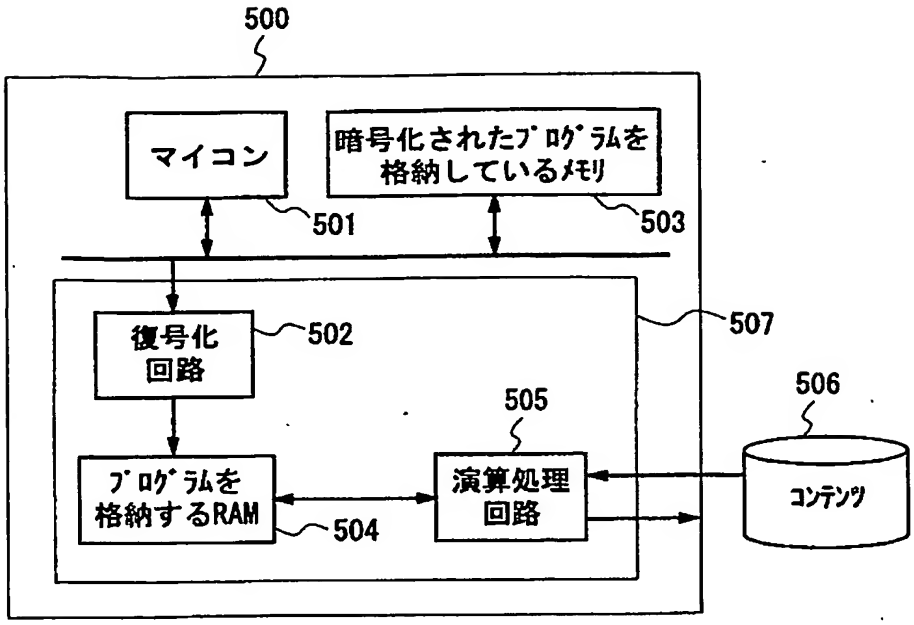
【図３】


300
マイコン
暗号化されたﾌﾟﾛｸﾞﾗﾑを
格納しているﾒﾓﾘ
301
303
復号化
回路
302
308
305
307
ﾌﾟﾛｸﾞﾗﾑを
格納するRAM
304
演算処理
回路
ｺﾝﾃﾝﾂ
制御回路
306

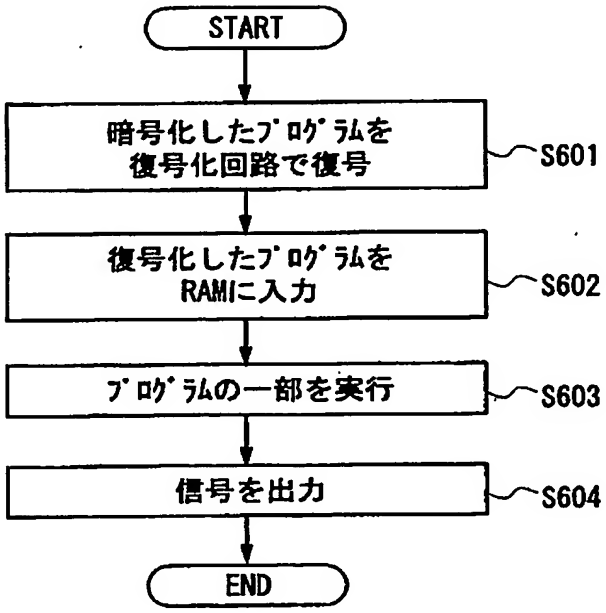
【図４】


START
暗号化したﾌﾟﾛｸﾞﾗﾑを
復号化回路で復号
S401
復号化したﾌﾟﾛｸﾞﾗﾑを
RAMに入力
S402
制御回路から
特定ｱﾄﾞﾚｽを読み出し
S403
特定ｱﾄﾞﾚｽを
外部に読み出してﾁｪｯｸ
S404
END

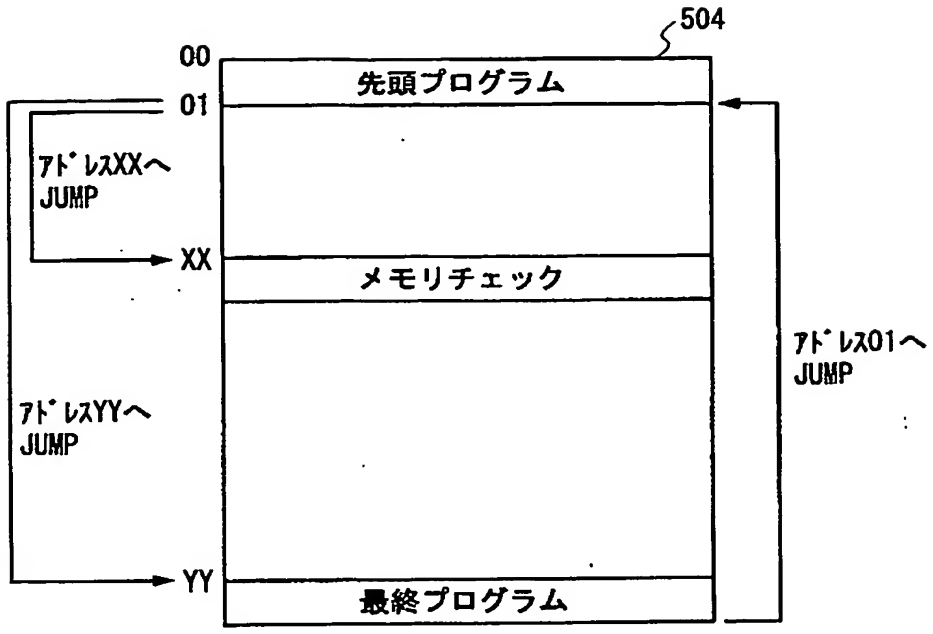
【図５】


500
マイコン
暗号化されたﾌﾟﾛｸﾞﾗﾑを
格納しているﾒﾓﾘ
501
503
復号化
回路
502
507
506
505
ﾌﾟﾛｸﾞﾗﾑを
格納するRAM
504
演算処理
回路
ｺﾝﾃﾝﾂ

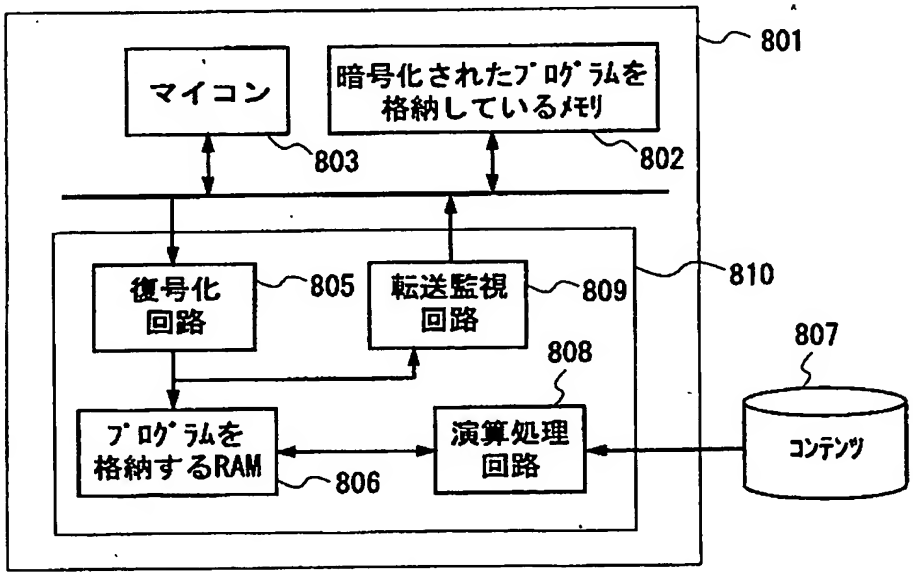
【図６】


START
暗号化したﾌﾟﾛｸﾞﾗﾑを
復号化回路で復号
S601
復号化したﾌﾟﾛｸﾞﾗﾑを
RAMに入力
S602
ﾌﾟﾛｸﾞﾗﾑの一部を実行
S603
信号を出力
S604
END

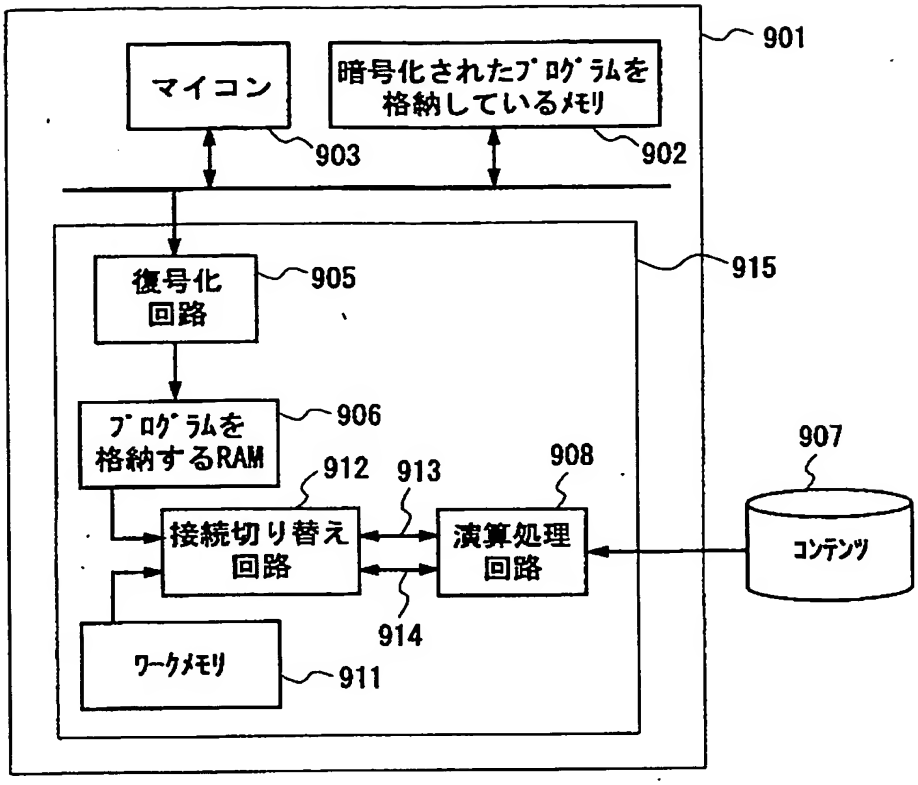
【図７】


504
00
先頭プログラム
01
ｱﾄﾞﾚｽXXへ
JUMP
XX
メモリチェック
ｱﾄﾞﾚｽ01へ
JUMP
ｱﾄﾞﾚｽYYへ
JUMP
YY
最終プログラム

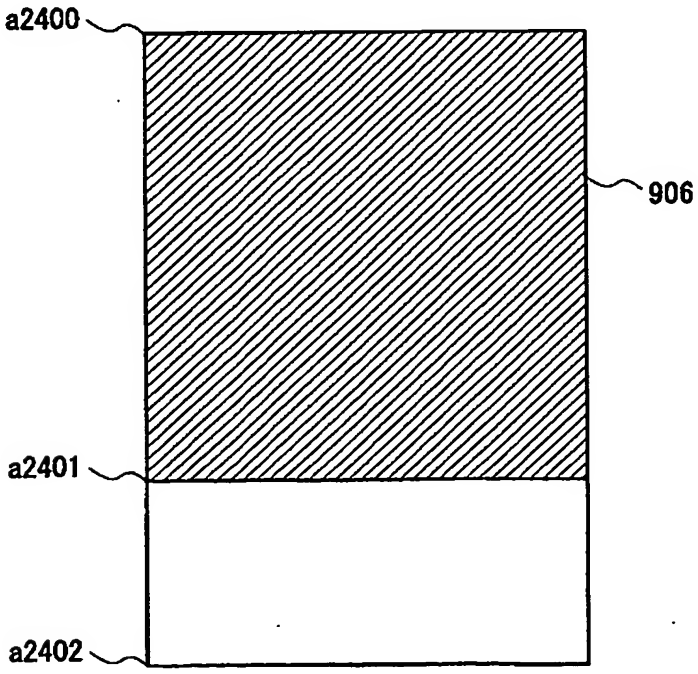
【図８】


801
マイコン
暗号化されたﾌﾟﾛｸﾞﾗﾑを
格納しているﾒﾓﾘ
803
802
復号化
回路
805
転送監視
回路
809
810
807
808
ﾌﾟﾛｸﾞﾗﾑを
格納するRAM
806
演算処理
回路
ｺﾝﾃﾝﾂ

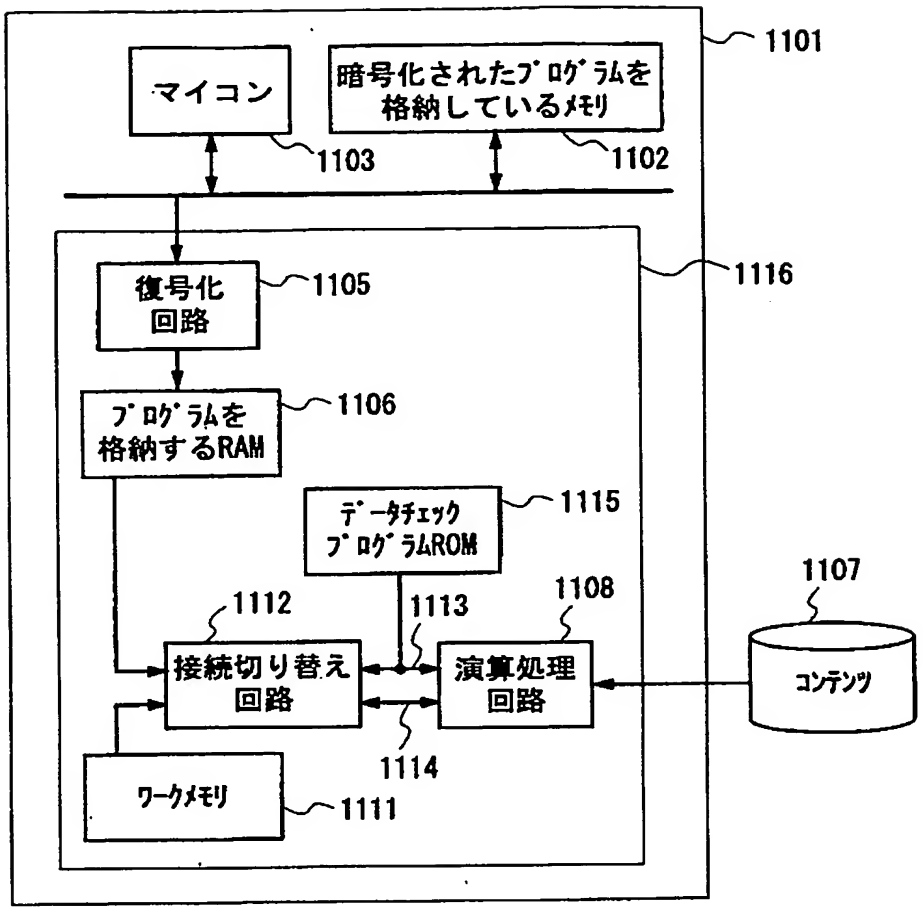
【図９】


901
マイコン
暗号化されたﾌﾟﾛｸﾞﾗﾑを格納しているﾒﾓﾘ
903
902
915
復号化回路
905
ﾌﾟﾛｸﾞﾗﾑを格納するRAM
906
907
912
913
908
接続切り替え回路
演算処理回路
ｺﾝﾃﾝﾂ
914
ﾜｰｸﾒﾓﾘ
911

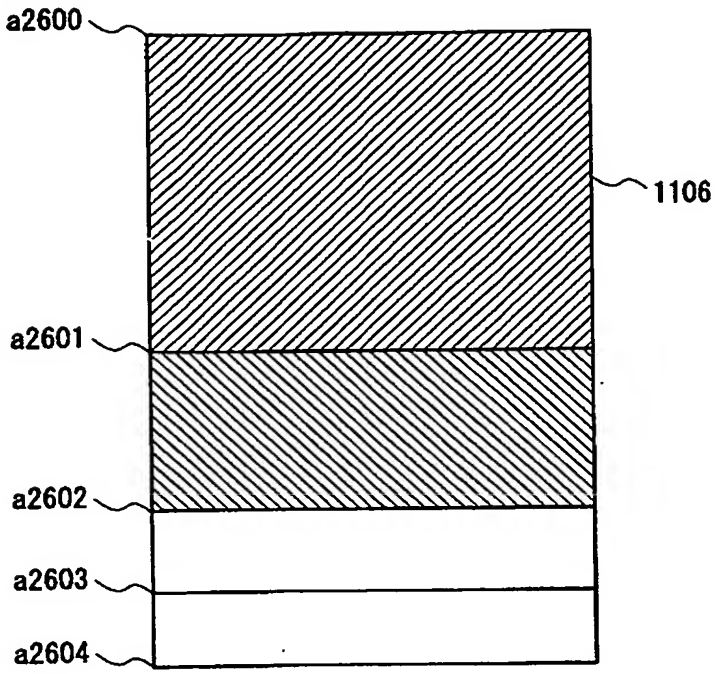
【図１０】


a2400
906
a2401
a2402

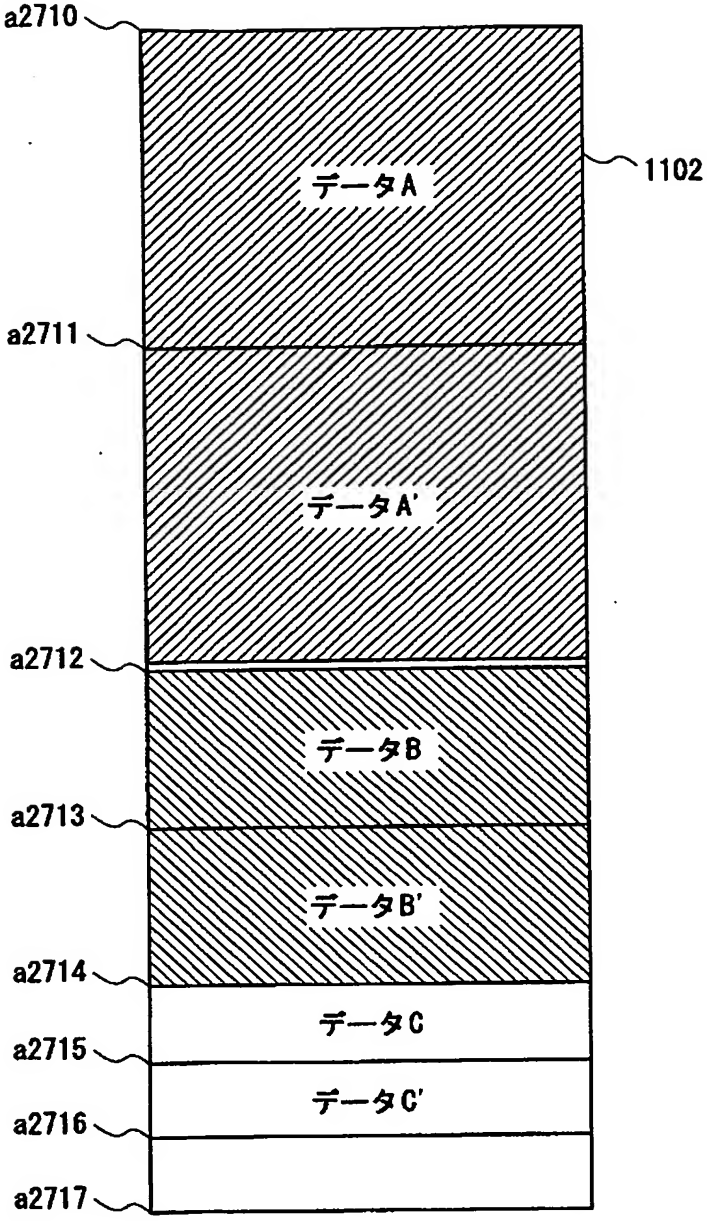
【図１１】


1101
マイコン
暗号化されたﾌﾟﾛｸﾞﾗﾑを格納しているﾒﾓﾘ
1103
1102
1116
復号化回路
1105
ﾌﾟﾛｸﾞﾗﾑを格納するRAM
1106
ﾃﾞｰﾀﾁｪｯｸﾌﾟﾛｸﾞﾗﾑROM
1115
1107
1112
1113
1108
接続切り替え回路
演算処理回路
コンテンツ
1114
ワークメモリ
1111

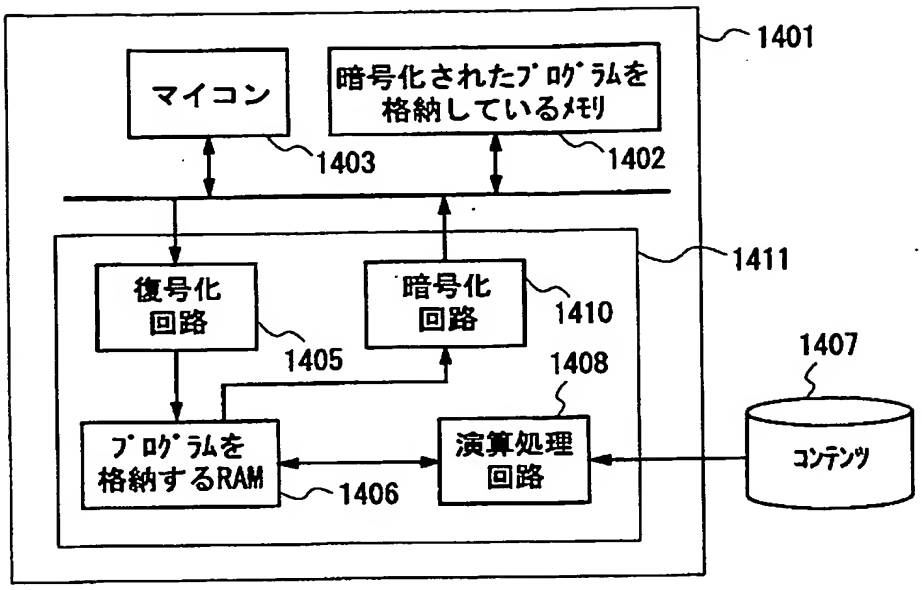
【図１２】



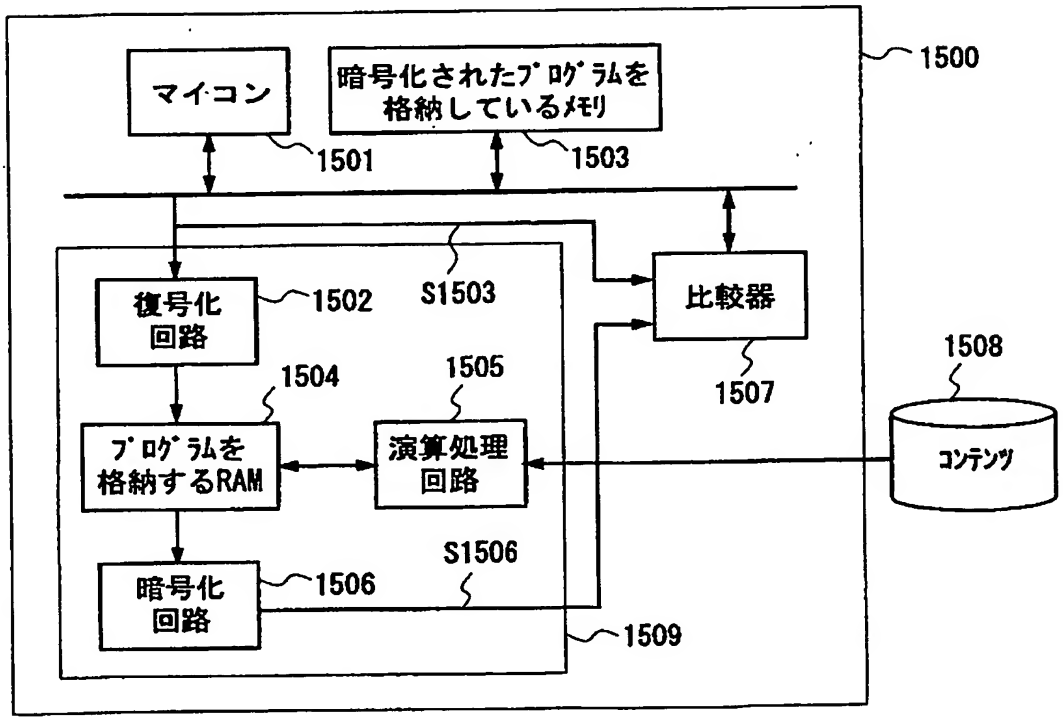
【図１３】


a2710
データA
1102
a2711
データA'
a2712
データB
a2713
データB'
a2714
データC
a2715
データC'
a2716
a2717

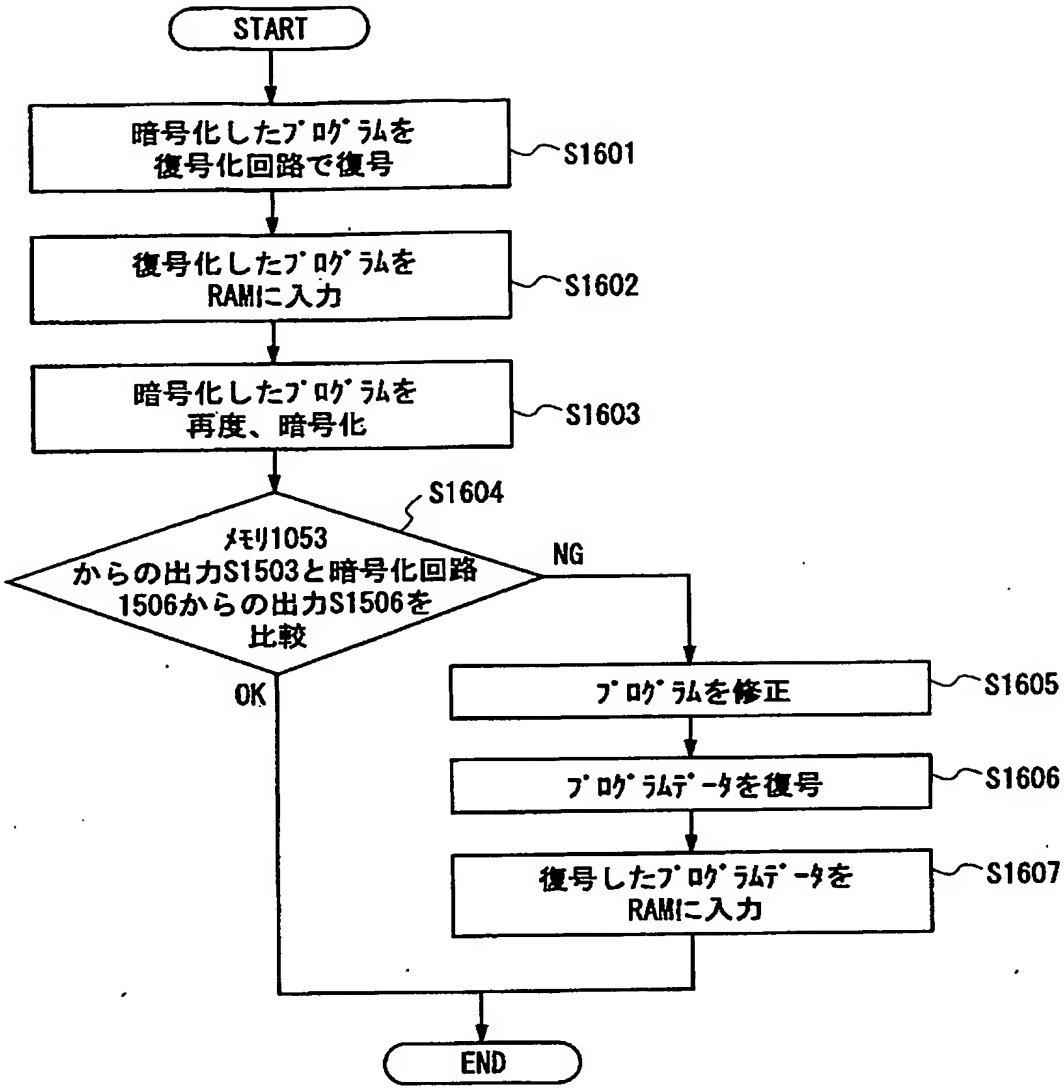
【図１４】


1401
マイコン
暗号化されたﾌﾟﾛｸﾞﾗﾑを格納しているﾒﾓﾘ
1403
1402
1411
復号化回路
暗号化回路
1410
1405
1408
1407
ﾌﾟﾛｸﾞﾗﾑを格納するRAM
1406
演算処理回路
ｺﾝﾃﾝﾂ

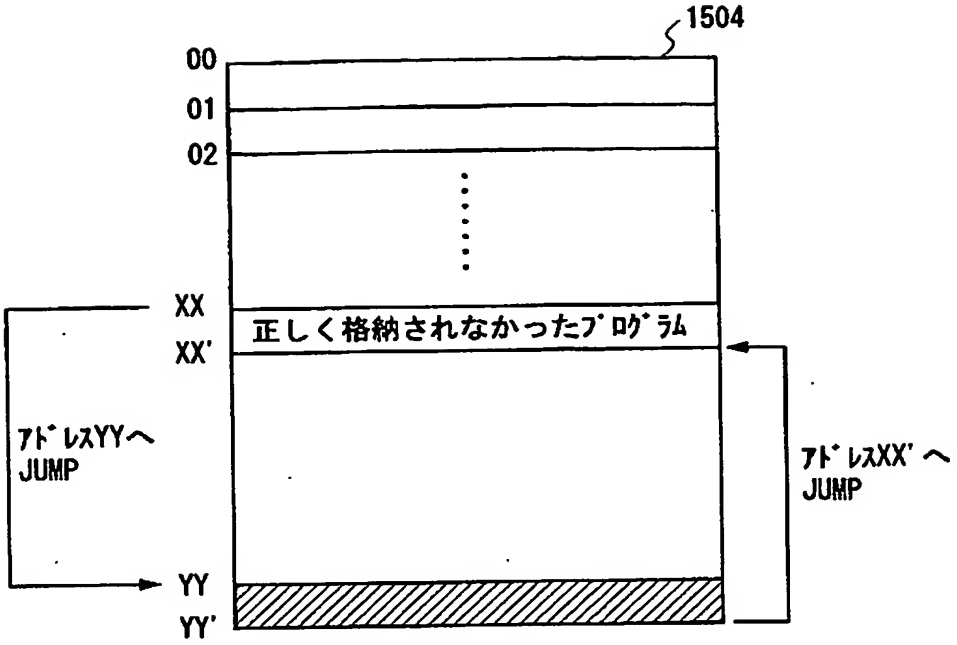
【図１５】


1500
マイコン
暗号化されたﾌﾟﾛｸﾞﾗﾑを格納しているﾒﾓﾘ
1501
1503
復号化回路
1502
S1503
比較器
1507
1508
1504
1505
ﾌﾟﾛｸﾞﾗﾑを格納するRAM
演算処理回路
ｺﾝﾃﾝﾂ
S1506
暗号化回路
1506
1509

【図１６】


START
暗号化したﾌﾟﾛｸﾞﾗﾑを
復号化回路で復号
S1601
復号化したﾌﾟﾛｸﾞﾗﾑを
RAMに入力
S1602
暗号化したﾌﾟﾛｸﾞﾗﾑを
再度、暗号化
S1603
S1604
ﾒﾓﾘ1053
からの出力S1503と暗号化回路
1506からの出力S1506を
比較
NG
OK
ﾌﾟﾛｸﾞﾗﾑを修正
S1605
ﾌﾟﾛｸﾞﾗﾑﾃﾞｰﾀを復号
S1606
復号したﾌﾟﾛｸﾞﾗﾑﾃﾞｰﾀを
RAMに入力
S1607
END

【図１７】


1504
00
01
02
XX
XX'
正しく格納されなかったﾌﾟﾛｸﾞﾗﾑ
ｱﾄﾞﾚｽYYへ
JUMP
ｱﾄﾞﾚｽXX'へ
JUMP
YY
YY'

【書類名】　要約書

【要約】

【課題】　ＤＳＰやＣＰＵなどの演算処理ユニットのプログラムを外部からダウンロードする半導体集積回路装置において、半導体集積回路内にダウンロードした、第三者に漏洩したくない機密情報である書き換えプログラムを、その機密を保持しながら該書き換えプログラムが正しくダウンロードできたか否かの確認を可能とする半導体集積回路装置を提供する。

【解決手段】　ダウンロードした書き換えプログラムの内容を検証する回路、及び／またはダウンロードした書き換えプログラムの内容を検証するプログラムを備える。

【選択図】　図１５

特願２００２－１７４８８３

出　願　人　履　歴　情　報

識別番号　　［０００００５８２１］

１．変更年月日　　１９９０年　８月２８日
［変更理由］　　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社